A FEW FACTS REGARDING NUMBER THEORY

LARRY SUSANKA

Contents

Date: October 13, 2018.

1. **Notation.**

To get started, we assume given the set of integers $\mathbb{Z}$, sometimes denoted

$$\{\dots, -2, -1, 0, 1, 2, \dots\}.$$

We assume that the reader knows about the operations of addition and multiplication on integers and their basic properties, and also the usual order relation on these integers.

In particular, the operations of addition and multiplication are commutative and associative, there is the distributive property of multiplication over addition, and $mn = 0$ implies one (at least) of m or n is 0.

The set $\mathbb{N}$ consists of the non-negative integers.

All lower case individual variable symbols referred to in a mathematical discussion such as $a, b, c, d, r, s, t, x, y, p, q, \dots$ will denote integers.

Any sets to which we refer will be subsets of $\mathbb{Z}$, and will be denoted by capitol letters such as S, T or V.

We presume you have heard of and understand the arithmetic of the rational numbers but will never refer to rational numbers except through an explicit ratio p/q of integers. Rational numbers are not "first-class" entities in our discussion. We say two representations p/q and m/n refer to the same rational number exactly when $pn = qm$, and in that case write $p/q = m/n$. If a rational number has representation $m/1$ we identify that rational number with the integer m.

For the sake of brevity we may sometimes use the following symbols, which are in common usage among math folk:

$\exists$	"There Exists"
$\exists!$	"There Exists a Unique" or "There Exists One and Only One"
$\forall$	"For All"
$\mid$	"Divides"
$\nmid$	"Does Not Divide"
$\subset$	"Is a Subset of "
$\in$	"Is an Element of " or "In"
$\Rightarrow$	"Implies "
$\Leftrightarrow$	"Implies and is Implied By" or "If and Only If"
s.t.	"Such That"
$\varnothing$	"the Empty Set"
$\square$	"End of Proof" or "Quod Erat Demonstrandum" or "Q.E.D."

Much of the content of this collection of notes is adapted from the very readable Burton *Elementary Number Theory* [Bur07] and the classic Hardy and Wright *An Introduction to the Theory of Numbers* [HW79], while expansion upon basic algebra facts can be found in Herstein *Topics in Algebra* [Her75]. Those authors are not responsible for any misinterpretations or errors or typos which the reader may find herein.

2. **Well Ordering and Induction.**

We list several tools upon which all our work rests. The first four are (close to) defining properties of the integers. The next two are proved by induction. The last involves useful and "obvious" properties of the order relation among integers.

You may assume the first five results in this section if you wish. Up to Section 23 (where you do calculations but must accept some statements on faith) declarative statements in the text and theorems, lemmas, propositions and corollaries are all to be proven or justified by the interested student. That includes filling any lacunae in arguments or proofs presented in the text.

Few proofs are given explicitly in the first few sections of text but later, as the results become more difficult, proofs (or outlines of proofs) are generally provided.

2.1. ***Theorem.*** *The* ***Well Ordering Principle****:*
Every nonempty set $S \subset \mathbb{N}$ contains a least element.

2.2. ***Theorem. Archimedean Order Property****:*
$\forall a, b \in \mathbb{N}$ *with* $a > 0$ $\exists!$ *least* n *s.t.* $an > b$.

2.3. ***Theorem. Finite Induction (I)****:*
If $S \subset \mathbb{N}$ *and* $0 \in S$ *and* $(k \in S \Rightarrow k + 1 \in S)$ *then* $S = \mathbb{N}$.

2.4. ***Theorem. Finite Induction (II)****:*
If $S \subset \mathbb{N}$ *and* $0 \in S$ *and* (*whenever* $k > 0$ *and* $j \in S \, \forall \, 0 \leq j < k$ *then* $k \in S$)
then $S = \mathbb{N}$.

2.5. ***Theorem.*** *Suppose a, b are positive integers and m is an integer.*
(i) $a \leq b \Leftrightarrow -a \geq -b$.
(ii) $a \leq b \Leftrightarrow a + m \leq b + m$.
(iii) $ab \geq am \Leftrightarrow b \geq m$.
(iv) If $m = ab$ *then both* $a \leq m$ *and* $b \leq m$. *And if* $a > 1$ *then* $b < m$.
(v) If $\varnothing \neq S$ *and* $S \subset \mathbb{N}$ *and* $\exists n \in \mathbb{N}$ *s.t.* $s \leq n \; \forall s \in S$
then S contains a largest member.

2.6. ***Theorem. The Binomial Theorem****:*
If $n > 0$ *then* $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *where* $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$.

2.7. ***Theorem. The Division Algorithm****:*
$\forall a, b$ *with* $b > 0$ $\exists! \, r, q$ *for which* $a = bq + r$ *and* $0 \leq r < b$.

3. **Intervals of Integers.**

3.1. **Definition**. An **interval of integers** is a set of the form

$$I_{j,k} = \{\, j + t \mid 0 \leq t < k \,\} \quad \text{for positive integer } k \text{ and any integer } j.$$

We will use $\Pi_{j,k}$ to denote the product of the members of $I_{j,k}$. This might be represented (imprecisely) as

$$\Pi_{j,k} = j\,(j+1)\,(j+2)\,\cdots\,(j+k-1).$$

3.2. **Remark**. $\Pi_{1,k}$ is the number often indicated by $k!$ and for positive j the binomial coefficient $\binom{j+k-1}{j-1}$ is $\Pi_{j,k}/\Pi_{1,k}$.

We would like to conclude that the ratio $\Pi_{j,k}/\Pi_{1,k}$ is an integer for *any* j and positive k. In our remark here we restrict attention to positive j.

The ratio is obviously an integer if either j or k are 1.

If $\Pi_{j,k}/\Pi_{1,k}$ fails to be an integer then it fails to be an integer for some least k and, for that k, some least j, both of which must exceed 1.

We are assuming, by this, that both

$$\frac{j\,(j+1)\,\cdots\,(j+k-2)}{(k-1)!} \quad \text{and}$$

$$\frac{(j-1)\,j\,(j+1)\,\cdots\,(j+k-2)}{k!} = \left(\frac{j-1}{k}\right)\frac{j\,(j+1)\,\cdots\,(j+k-2)}{(k-1)!}$$

are whole numbers. But if that is true then

$$\begin{aligned}
\Pi_{j,k}/\Pi_{1,k} &= \frac{j\,(j+1)\,\cdots\,(j+k-1)}{k!} \\
&= \frac{j\,(j+1)\,\cdots\,(j+k-2)}{(k-1)!}\left(\frac{j+k-1}{k}\right) \\
&= \frac{j\,(j+1)\,\cdots\,(j+k-2)}{(k-1)!}\left(\frac{j-1}{k}\right) + \frac{j\,(j+1)\,\cdots\,(j+k-2)}{(k-1)!}
\end{aligned}$$

is the sum of two integers and therefore, itself, an integer. This is contrary to assumption. We conclude the ratio must be an integer for all positive j and k.

This implies (if you have no other way of seeing this) that the coefficients in the binomial theorem are integers.

3.3. ***Proposition.*** *$\Pi_{j,k}/\Pi_{1,k}$ is an integer for any j and any positive k.*

4. **Greatest Common Divisor and Least Common Multiple.**

4.1. **Definition**. We write $a|b$ (read as " a divides b") when $a \neq 0$ and $b = ka$ for some k. We write $a \nmid b$ when $a \neq 0$ and $b = ka + r$ for some k and r with $0 < r < |a|$.

4.2. **Remark**. (i) The values of k and r in the definition above are unique for each nonzero a and b.
(ii) If $a \neq 0$ then for each b either $a|b$ or $a \nmid b$.
(iii) If $a|b$ and $b|a$ then $a = \pm b$.

4.3. **Definition**. A nonempty set S is called an **ideal** if $xs_1 + ys_2 \in S$ whenever s_1 and s_2 are in S and any $x, y \in \mathbb{Z}$. We say "S is closed under linear combinations with coefficients in $\mathbb{Z}$."

The set $\{\, 0 \,\}$ is obviously an ideal, called the trivial ideal. $\mathbb{Z}$ itself is an ideal. If n is any integer the set $n\mathbb{Z}$ defined to be $\{\, nx \mid x \in \mathbb{Z} \,\}$ is an ideal, called the ideal generated by n.

4.4. ***Lemma.*** *(i) If n is any integer and S is an ideal the set nS defined to be $\{\, nx \mid x \in S \,\}$ is an ideal.*
(ii) If T is another ideal, the set $S + T$ defined to be $\{\, x + y \mid x \in S,\, y \in T \,\}$ is an ideal and $S + T = T + S$.
(iii) If V is another ideal then $S + (V + T) = (S + V) + T$.
(iv) If $T \subset V$ then $V + T = V$.
(v) For nonzero i and j, $j\mathbb{Z} \subset k\mathbb{Z} \Leftrightarrow k|j$.
(vi) $j\mathbb{Z} + k\mathbb{Z} = k\mathbb{Z} \Leftrightarrow j\mathbb{Z} \subset k\mathbb{Z}$.

4.5. ***Theorem.*** *If S is a nontrivial ideal there exists a unique positive n for which $S = n\mathbb{Z}$.*

Proof. Let n be the least positive member of S. Obviously $n\mathbb{Z} \subset S$. Suppose $k \in S$. So there are numbers j and r with $0 \leq r < n$ with $k = jn + r$. But then $r = k - jn \in S$, and the minimality of n among such numbers forces $r = 0$. So $S \subset n\mathbb{Z}$. □

4.6. **Definition**. For ideals S and T define ST to be $\{\, st \mid s \in S \text{ and } t \in T \,\}$.

4.7. ***Corollary.*** *If S and T are ideals so is ST. In fact, if $S = j\mathbb{Z}$ and $T = k\mathbb{Z}$ then $ST = (jk)\mathbb{Z} = j(k\mathbb{Z})$.*

4.8. **Definition**. Suppose a, b are not both 0. We write $d = \boldsymbol{gcd(a, b)}$ when $d|a$ and $d|b$ and whenever $c|a$ and $c|b$ then $c|d$. The number d is called the **greatest common divisor (short form: GCD)** of a and b. Greatest common divisors exist.

4.9. ***Theorem.*** *$d = gcd(a, b)$ is the least positive integer that can be formed as $d = ax + by$ for $x, y \in \mathbb{Z}$. Therefore $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, and whenever $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$ then $n = \pm d$.*

4.10. **Remark**. Some texts define $gcd(a, b)$ for integers a and b in a slightly different way: as the positive integer d for which $d|a$ and $d|b$ and if $c|a$ and $c|b$ then $c \leq d$. The two definitions are equivalent.

4.11. ***Proposition.*** *If $b \neq 0$, $gcd(a, b) = |b| \Leftrightarrow a = bm$ for some m.*

4.12. **Definition**. Suppose a, b are not both 0. The numbers a and b are said to be **relatively prime** or, synonymously, **coprime** whenever $gcd(a, b) = 1$.
This is equivalent to the condition $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

4.13. **Definition**. Suppose $a_1, \ldots, a_k$ are all nonzero for some $k > 2$. We write $d = \boldsymbol{gcd(a_1, \ldots, a_k)}$ when $d|a_i \forall i$ and whenever $c|a_i \forall i$ then $c|d$. There actually is a number of this kind for every finite set of a_i, and this number d is called the **greatest common divisor** of these a_i.

4.14. ***Theorem.*** *$d = gcd(a_1, \ldots, a_k)$ is the least positive integer that can be formed as $d = a_1x_1 + \cdots + a_kx_k$ for $x_i \in \mathbb{Z}$. This is equivalent to the condition $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} = d\mathbb{Z}$.*

4.15. ***Proposition.*** *Suppose $a_1, \ldots, a_k$ are all nonzero for some $k > 2$. $gcd(a_1, \ldots, a_k) = gcd(gcd(a_1, \ldots, a_{k-1}), a_k)$.*

4.16. ***Lemma.*** *(i) For positive d, $gcd(a, b) = d$ if and only if $d|a$ and $d|b$ and $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

(ii) If $gcd(a, b) = ax + by$ then $gcd(x, y) = 1$.

*(iii) **Euclid's Lemma**: If $a|bc$ and $gcd(a, b) = 1$ then $a|c$.*

(iv) If $a|c$ and $b|c$ and $gcd(a, b) = 1$ then $ab|c$.

(v) If $k > 0$ and a, b are not both 0 then

$$gcd(ka, kb) = k\, gcd(a, b).$$

4.17. ***Theorem.*** *If $a > b > r \geq 0$ and $a = bk + r$ then $gcd(a, b) = gcd(r, b)$.*

4.18. **Remark**. Iterating the calculation identified in Theorem 4.17 provides a means of producing $d = gcd(a, b)$ which can also be used to calculate the x, y pair for which $ax + by = d$. This process is called the **Euclidean Algorithm**, described in book VII of Euclid's[1] *Elements*.

As an example we produce $gcd(10600, 113)$.

Using long division we find, successively:

$$10600 = 113 \cdot 93 + 91, \quad 113 = 91 \cdot 1 + 22, \quad 91 = 22 \cdot 4 + 3, \quad 22 = 7 \cdot 3 + 1.$$

This means

$$gcd(10600, 113) = gcd(113, 91) = gcd(91, 22) = gcd(22, 3) = gcd(3, 1)$$

at which point the process terminates by repetition at a value of 1.

But working backwards (which takes fewer multiplication steps than the number of divisions used above) we also have

$$\begin{aligned} 1 &= 22 - 7 \cdot 3 = 22 - 7 \cdot (91 - 22 \cdot 4) = 29 \cdot 22 - 7 \cdot 91 \\ &= 29 \cdot (113 - 91) - 7 \cdot 91 = 29 \cdot 113 - 36 \cdot 91 \\ &= 29 \cdot 113 - 36 \cdot (10600 - 113 \cdot 93) = (29 + 36 \cdot 93) \cdot 113 - 36 \cdot 10600 \\ &= 3377 \cdot 113 - 36 \cdot 10600. \end{aligned}$$

which produces 1 as the required combination of 113 and 10600.

4.19. **Definition**. If a and b are nonzero we write $\boldsymbol{lcm(a, b)} = m$ if $m > 0$ and $a|m$ and $b|m$ and whenever $a|c$ and $b|c$ then $m|c$. The number m is called the **least common multiple (shorter form: LCM)** of a and b.

4.20. ***Proposition.*** *If a and b are nonzero then $lcm(a, b) = \frac{ab}{gcd(a,b)}$.*

4.21. ***Corollary.*** *For nonzero a and b, $lcm(a, b) = ab \Leftrightarrow gcd(a, b) = 1$.*

[1]Euclid of Alexandria circa 300 BCE reputedly assembled and organized and improved the work of previous mathematicians in *The Elements*. Earlier mathematicians who probably contributed included Pythagoras circa 570-495 BCE, Hippocrates of Chios 470-410 BCE and Eudoxus of Cnidus circa 408-355 BCE. It is the most successful text ever written, having been used continuously in one form or another for over 2000 years as the primary text for mathematical instruction in Europe and the Islamic countries.

5. **A Theorem of Lamé.**

Gabriel Lamé[2] showed that the Euclidean Algorithm will terminate at the greatest common divisor using a predictable, and manageably small, number of steps. This may be the first recorded example (1844) of "time to terminate" for an algorithm, a subject of vital importance today.

Before proving this result we define and discuss (a little) the **Fibonnaci**[3] **sequence**, used in the proof to follow.

This sequence is defined inductively by $F_0 = 0,\ F_1 = 1$ and generally, for $n > 1$, by $F_{n+1} = F_n + F_{n-1}$. Thus $F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13$ and so on.

The following lemma guarantees that the Fibonacci sequence gains *at least* one (base 10) digit in length every five steps along the sequence.

5.1. ***Lemma.*** *$F_{n+5} > 10 \cdot F_n$ for all $n \geq 2$.*

Proof. $F_7 = 13 > 10 \cdot F_2 = 10$. So we have the result for $n = 2$.

And if $n \geq 3$ we have

$$\begin{aligned} F_{n+5} &= F_{n+4} + F_{n+3} = F_{n+3} + F_{n+2} + F_{n+3} = 2(F_{n+2} + F_{n+1}) + F_{n+2} \\ &= 3 \cdot F_{n+2} + 2F_{n+1} = 3(F_{n+1} + F_n) + 2F_{n+1} = 5F_{n+1} + 3F_n \\ &= 8F_n + 5F_{n-1}. \end{aligned}$$

Since the sequence is non-decreasing we know $F_n = F_{n-1} + F_{n-2} \leq 2F_{n-1}$ and the result is proved. □

5.2. ***Proposition. Lamé's Theorem***
Using the Euclidean algorithm as above to produce the greatest common divisor of two numbers terminates after no more than 5 *times the number of digits (base* 10*) of the shorter of the two numbers.*

Proof. Suppose x and y are positive and $x > y$ and the Euclidean algorithm *requires* exactly n steps to produce the greatest common divisor of these two numbers.

---

[2]Gabriel Lamé 1795-1870.

[3]Leonardo Fibonnaci, 1175-1250, who introduced his eponymous numbers and the Hindu-Arabic number system in general to Europeans and studied their properties, was an Italian mathematician with extensive contact with the Arabic world through his travels in Northern Africa.

Letting $x = x_n$ and $y = x_{n-1}$ we reproduce this sequence of divisions below.

$$\begin{aligned} x_n &= m_n \cdot x_{n-1} + x_{n-2} \\ x_{n-1} &= m_{n-1} \cdot x_{n-2} + x_{n-3} \\ &\vdots \\ x_3 &= m_3 \cdot x_2 + x_1 \\ x_2 &= m_2 \cdot x_1 + x_0 \\ x_1 &= m_1 \cdot x_0 \end{aligned}$$

In each line but the last, $x_k,\ x_{k-1},\ x_{k-2}$ are in strictly decreasing order with m_k at least 1. In the last line the least common denominator, x_0 is less than x_1 and m_1 is at least 2.

That means that the smallest possible numbers that would reproduce a list of equations like this are Fibonnaci numbers with $x_k = F_{k+2}$ for $0 \leq k \leq n$.

So x_5 (if there is a term like this) must have at least one more digit than x_0, and x_{10} must have at least one more digit than x_5 and so on. Since x_0 itself has at least one digit, the complete number of divisions on the list, n, cannot exceed 5 times the number of digits of x_{n-1} as stated in the proposition. □

We note that the Fibonacci numbers $F_{12} = 144$ and $F_{11} = 89$ provide an example where the Euclidean algorithm does require 10 divisions to achieve the last line of the calculation, showing that the number 5 of the proposition cannot be improved upon.

6. **Linear Diophantine Equations.**

6.1. **Definition**. A **Diophantine Equation** is an equation that is to be solved for integer values of any variables involved.

6.2. ***Proposition.*** *The Diophantine*[4] *Equation $ax + by = c$ in variables x and y has a solution exactly when $gcd(a, b) = d|c$.*

In that case, and if x_0, y_0 is any particular solution, all others can be found among the paired numbers

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t \quad \textit{for any integer } t$$

which are (each pair) solutions for every t.

[4]Diophantus of Alexandria circa 200-300 AD

6.3. **Remark**. If Diophantine Equation $ax+by = c$ has a solution then those solutions are exactly the solutions of $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ and this last equation is of the form $rx + sy = m$ where $gcd(r, s) = 1$.

So if you can find $\overline{x}$ and $\overline{y}$ (by the Euclidean Algorithm, for instance) so that $r\overline{x} + s\overline{y} = 1$ then a particular solution to our original equation will be given as $x_0 = m\overline{x}$ and $y_0 = m\overline{y}$. All other solutions can be found as $x = mx_0 + st$, $y = my_0 - rt$ as prescribed in Proposition 6.2.

As another point, we have a method for finding a particular solution to $ax + by = d$ where $d = gcd(a, b)$. This tells us about all the others. The x values all differ from each other by $\frac{b}{d}t$ while the corresponding y values differ by $\frac{-a}{d}t$ for the same integer t. In particular, if a and b are nonzero we can always choose the value of x to satisfies $0 \leq x < \frac{b}{d}$, and there is only one solution for which the x value satisfies that inequality.

7. **Prime Factorization.**

7.1. **Definition**. A number $p > 1$ is called **prime** if

$$a|p \Rightarrow a = \pm 1 \quad \text{or} \quad a = \pm p.$$

A number exceeding 1 that is not prime is called **composite**. A negative number is called composite if its negative, which is positive, is composite.

Note that the numbers 0, -1 and 1 are neither prime nor composite.

7.2. ***Proposition.*** *If p is prime then for any a,*

$$gcd(a, p) = 1 \text{ or } gcd(a, p) = p.$$

7.3. ***Lemma.*** *If p is prime and $p|ab$ then $p|a$ or $p|b$.*

7.4. ***Corollary.*** *If p is prime and $p|\, q_1 \cdots q_k$ then $p|q_i$ for some i.*
If all the q_i are themselves prime then $p = q_i$ for some i.

The following theorem can now be proved by induction.

7.5. ***Theorem. The Fundamental Theorem of Arithmetic***
Every positive integer has a unique factorization as a product of prime powers, where the primes are listed in order of increasing size.

This result, when prime power exponents are 1, was proved in books VII and IX of Euclid's *Elements*.

7.6. **Remark**. There are an infinitude of distinct primes.[5]

[5]What do you think the word "infinitude" means here?

8. Int_n, mod n Arithmetic and Fermat's Little Theorem.

8.1. **Definition**. When $n > 1$ we write $\boldsymbol{a \equiv b \mod n}$ to mean $a = b + kn$ for some k. This is read aloud as "a is **congruent** to b mod n." This is equivalent to the condition: $n|(a - b)$.

n is called the **modulus** of the congruency.

An assertion that several numbers are congruent can be combined in a single line using only one mod n indication.

$$a \equiv b \equiv c \mod n$$

may be preferred to

$$a \equiv b \mod n \quad \text{and} \quad b \equiv c \mod n.$$

In contrast, the expression

$$a = b \equiv c \mod n$$

means that a is numerically equal to b which is congruent to c mod m.

If $0 \leq r < n$ and $b \equiv r \mod n$ the number r is called the **residue**[6] of b mod n. Each number has one and only one residue for each modulus.

Sometimes it is convenient to refer to $c \mod n$ as a single number, and when we do it is to this residue that we refer.

We say numbers are **distinct** mod n if they have different residues mod n. We say numbers are **equivalent mod n** if they have the same residues[7]. We say a number satisfying some condition is **unique mod n** if all numbers satisfying that condition have the same residue.

8.2. ***Lemma.*** *If $a \equiv b \mod n$ and $c \equiv d \mod n$*
then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.

8.3. ***Lemma.*** *Suppose $d = gcd(c, n)$.*
(i) $ca \equiv cb \mod n$ exactly when $a \equiv b \mod \frac{n}{d}$.
(ii) $ca \equiv b \mod n$ exactly when $d|b$ and $\frac{c}{d} \cdot a \equiv \frac{b}{d} \mod \frac{n}{d}$.

8.4. **Remark**. Lemma 8.2 implies that if $a \equiv b \mod n$ then $a^k \equiv b^k \mod n$ for any positive k and, in fact, $f(a) \equiv f(b) \mod n$ for any polynomial f with integer coefficients.

Lemma 8.3 (i) tells us when/how we can "cancel" common factor c in a statement asserting congruency involving mod n arithmetic to obtain an equivalent congruency. If $gcd(c, n) = 1$, you can *always* do it.

Also if m is prime, $ab \equiv 0 \mod m \Rightarrow a \equiv 0 \mod m$ or $b \equiv 0 \mod m$. If m is composite you *cannot* draw this conclusion.

---

[6] In some sources this is called the least non-negative residue.

[7] "Equivalent mod n" and "congruent mod n" are widely used synonymous expressions.

8.5. **Definition**. We define, for integer m and nonzero k the set

$$[\boldsymbol{m}]_{\boldsymbol{k}} = m + k\mathbb{Z} = \{\, m + kn \mid n \in \mathbb{Z} \,\}.$$

Each integer is in one and only one of the sets

$$[0]_k, \quad [1]_k, \quad [2]_k, \quad \ldots, \quad [k-1]_k$$

and each of these sets consists of numbers with shared residue mod k. The sets are called the **congruency or residue (synonymous) classes mod $\boldsymbol{k}$**. Sometimes they are also called ***k*-congruency classes**. Whatever you call them, there are k of these sets of integers and their collective, the set of these classes, will be denoted[8] $\boldsymbol{Int_k}$.

The statement $[a]_k = [b]_k$ is identical in meaning to $a \equiv b \mod k$.

8.6. **Definition**. Given residue classes $[m]_k$ and $[n]_k$ define

$$[m]_k + [n]_k = [m+n]_k \quad \text{and also} \quad [m]_k \cdot [n]_k = [m \cdot n]_k.$$

8.7. **Remark**. In view of Theorem 8.2, these operations don't depend on the representatives m and n chosen for the congruency classes: any equivalent numbers could have been chosen and would yield the same sum or product congruency classes[9]. These operations are associative and mod k multiplication distributes over mod k addition. Addition is commutative and there is an additive identity so Int_k with these two operations is an example of what mathematicians call a **ring**.

Since multiplication is also commutative, this ring is called commutative. Since there is a multiplicative identity this ring is called **unitary**. An integer m and the modulus k are relatively prime if and only if $[m]_k$ has a multiplicative inverse. Whenever $[m]_k \cdot [j]_k = [1]_k$ we will call m and j **mod k multiplicative inverses** (to each other.) If k is prime *every* nonzero member of Int_k has a multiplicative inverse and the only integers without mod k multiplicative inverses are the multiples of k.

A commutative unitary ring for which every nonzero element has a multiplicative inverse is called a **field**. The real numbers and the complex numbers and the rational numbers are fields, which do not concern us here. For prime k we have created *finite* fields.

8.8. ***Lemma.*** *If p is prime then $[a]_p[b]_p = [0]_p$ if and only if at least one of a or b is a multiple of p: that is, $[a]_p = [0]_p$ or $[b]_p = [0]_p$.*

---

[8]Many texts use $\mathbb{Z}/k\mathbb{Z}$ or $\mathbb{Z}_k$ to denote this collective. The former is ugly and the latter clashes with an identical notation for the k-adic integers, which we do not consider here.

[9]Any definition given for sets of integers by operations on a generic member of the set must be shown to be unambiguous: that the result is independent of *which* representative is picked. When this is true we say the operation or construction is **well defined.** Showing a definition given this way is well defined is not optional.

8.9. ***Theorem. Fermat's Little Theorem***[10]***:***
If p is prime then $a^p \equiv a \mod p$ for all a.

Proof. If a is 1 (or any multiple of p) the result is obvious.

Suppose we know the result for integer a. Then

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1$$

by the binomial theorem. p divides each middle term on the right, so

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \mod p.$$

The result now follows for all positive a by induction on a. The case of non-positive a is left to the reader. □

8.10. **Remark**. By this result, for prime p and any a we have $[a]_p^p = [a]_p$. An alternative phrasing is that the polynomial equation $X^p - X = 0$ has p distinct solutions in Int_p. Every member of Int_p satisfies that equation.

9. The Chinese Remainder Theorem.

9.1. ***Lemma.*** *The equation $ax \equiv b \mod n$ in variable x has a solution exactly when $d|b$ where $d = gcd(a, n)$. If it does have a solution then there are exactly d distinct mod n solutions. Each of these solutions is equivalent to the x component of one of the solution pairs*

$$x = x_0 + \frac{n}{d}t, \quad y = y_0 + \frac{a}{d}t \quad \text{for } t = 0, \ldots, d-1$$

where x_0, y_0 is any particular solution pair to the equation

$$\frac{a}{d}x - \frac{n}{d}y = \frac{b}{d}.$$

This particular solution can be found as suggested in Remark 6.3.

9.2. ***Corollary.*** *If $gcd(a, n) = 1$ the congruency $ax \equiv 1 \mod n$ has one solution mod n.*

9.3. **Remark**. Corollary 9.2 tells us that if a is relatively prime to n then $[a]_n$ has a multiplicative inverse. But if $gcd(a, n) \neq 1$ then $[a]_n$ does *not* have a multiplicative inverse.

[10]Pierre de Fermat 1607-1665. Strikingly, Fermat was a lawyer, not a professional mathematician. That makes his numerous contributions to precursor work for infinitesimal calculus, analytic geometry, probability, optics and, especially, number theory all the more impressive. At the time he did not publish, but letters containing his many results and sent to mathematician friends made his results known. The importance of his many contributions to number theory were not fully understood until the time of Euler, 80 years later.

9.4. ***Theorem. The Chinese Remainder Theorem:*** *Suppose $n_1, \ldots, n_k$ are pairwise relatively prime positive numbers and $a_1, \ldots, a_k$ are any nonzero numbers.*

Then the system of equations

$$x \equiv a_i \mod n_i \quad \textit{for } i = 1, \ldots, k$$

has a unique solution mod n, where $n = n_1 \cdots n_k$.

Proof. Let $N_j = n/n_j$ for each j. So $gcd(N_j, n_j) = 1$ for each j. So there is exactly one solution mod n_j for equation $N_j x \equiv 1 \mod n_j$ for each j. Let x_j denote this solution. Then

$$x = a_1 N_1 x_1 + \cdots + a_k N_k x_k$$

is a solution to the system of equations, as can be readily checked.

If $\overline{x}$ is another solution then n_j divides $x - \overline{x}$ for each j so n divides $x - \overline{x}$ and we have uniqueness mod n. □

9.5. **Remark**. This theorem was, apparently, first recorded some time around or after 400 AD in the work ***Sunzi Suanjing***, a title roughly translated as "Classic Mathematical Facts by Master Sun."[11]

In the Chinese Remainder Theorem it is necessary that the n_i be pairwise relatively prime. It is easy to produce systems with no solution otherwise.

10. $RelPrime_n$, Euler's Theorem and Gauss' Theorem.

10.1. **Definition**. For positive integer n define $\boldsymbol{RelPrime_n}$ to consist of those *nonzero* residue classes, members of Int_n, with residues which are relatively prime, or coprime, to n.

Every member of $RelPrime_n$ has a multiplicative inverse, and the product of two members of $RelPrime_n$ is also in $RelPrime_n$. But the sum of two members of $RelPrime_n$ might *not* be in $RelPrime_n$, even when n is prime.

For a given positive number n, $\boldsymbol{\phi(n)}$ is the number of positive numbers not exceeding n which are coprime to n: that is, $\phi(n)$ is the number of classes in $RelPrime_n$. For historical reasons ϕ is referred to as the Euler **totient function**.

So $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$ and so on.

[11]This is *not* the military strategist Sun Tzu, who authored "The Art of War" sometime around 500 BCE. Almost nothing is known about this mathematician, from which it is deduced that he was *not* a government official or from a family of high standing. The nature of the problems he solves in this work suggests he was, possibly, a Buddhist and interested in various social issues.

10.2. **Remark**. Obviously, if p is prime $\phi(p) = p - 1$. It is not hard to show that $\phi(p^k) = p^k - p^{k-1}$ for prime p and $k > 0$.

And if m and n exceed 1 and are relatively prime then $\phi(mn) = \phi(m)\phi(n)$.

To see this we explicitly count relatively prime integers as follows.

Arrange the numbers between 1 and mn in an n-row-by-m-column rectangle. Each column consists of those numbers in the array with identical mod m residue. So all but $\phi(m)$ of these columns may be immediately deleted from consideration, since the other columns have residues that share a nontrivial factor with m. Each remaining column has $\phi(n)$ numbers coprime, also, to n and the result follows.

10.3. ***Theorem.*** *For coprime m and n greater than 1 we have*

$$\phi(mn) = \phi(m)\phi(n)$$

This implies that if $n = p_1^{k_1}p_2^{k_2}\cdots p_j^{n_j}$ is the factorization of integer n (assumed to exceed 1) into the product of positive powers of distinct primes then:

10.4. ***Corollary.***

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_j^{k_j} - p_j^{k_j-1}).$$

10.5. **Remark**. $RelPrime_n$ with mod n multiplication has useful and interesting properties. For instance if $[a]_n$ is in $RelPrime_n$ the list

$$[a]_n, [a^2]_n, [a^3]_n, \ldots, [a^k]_n, \ldots$$

must begin to repeat at some smallest integer $k+1$ and since $[a]_n[b]_n = [ab]_n$ for any b it follows that $[a^k]_n = [1]_n$ and so $[a]_n[a^{k-1}]_n = [1]_n$.

So the mod n multiplicative inverse of $[a]_n$ is actually a power of $[a]_n$.

This smallest k is called the **order** of the element $[a]_n$, denoted $\boldsymbol{o_n(a)}$.

10.6. ***Theorem.*** *The order of any element of $RelPrime_n$ must divide $\phi(n)$.*

Proof. To see this examine the two lists

$$[ja]_n, [ja^2]_n, \ldots, [ja^k]_n \qquad [ta]_n, [ta^2]_n, \ldots, [ta^k]_n$$

for integers j and t relatively prime to n and where k is the order of $[a]_n$.

There are no repeated classes on either list, and if the first list shares even one member with the other list then they are the same list. And every member of $RelPrime_n$ is on one list. □

We have, immediately, the following result.

10.7. ***Corollary. Euler's[12] Theorem***
If $n \geq 2$ and $gcd(a, n) = 1$ then

$$a^{\phi(n)} \equiv 1 \mod n.$$

If n is prime then $\phi(n) = n - 1$ so $a^{n-1} \equiv 1 \mod n$ for every integer coprime to n: in particular, for all numbers between 1 and $n - 1$. However if n is composite and if $\phi(n)$ has a common factor t with $n - 1$ it is still possible that there could be an element $[a]_n \in RelPrime_n$ of order t, and if there is we have $a^{n-1} \equiv 1 \mod n$. So a "behaves as if" n is prime, since it satisfies one of the consequences it would *have* to satisfy if n *were* prime.

This effect can be extreme if $n - 1$ and $\phi(n)$ share many factors.

However if a and b are coprime to n and if $a^{n-1} \equiv 1 \mod n$ but $b^{n-1} \not\equiv 1 \mod n$ then $(a \cdot b)^{n-1} \not\equiv 1 \mod n$. So for every a that behaves, by this test, as if n is prime there will be a paired relatively prime integer $a \cdot b$ that *fails* to behave as if n is prime. The conclusion below follows.

10.8. ***Corollary.*** *If $n \geq 2$ and there exists a single $[b]_n \in RelPrime_n$ for which $b^{n-1} \not\equiv 1 \mod n$ then no more than half the elements of $RelPrime_n$ have order that divides $n - 1$.*

Recall that for positive integers m and n, $gcd(m, n) = d$ exactly when $gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

So if A_d is the number of positive integers m not exceeding n for which $gcd(m, n) = d$ we have $A_d = \phi\left(\frac{n}{d}\right)$. That means

$$n = \sum_{d|n} A_d = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{c|n} \phi(c)$$

where the sums are taken over positive divisors of n.

We have, therefore, proven one of *many* theorems due to Gauss[13]:

10.9. ***Theorem. Gauss' Theorem***

For positive n we have $$n = \sum_{c|n} \phi(c)$$

[12]Leonhard Euler 1707-1783
[13]Karl Friedrich Gauss 1777-1855

11. **Lagrange's Theorem and Primitive Roots.**

11.1. **Remark**. If $n = a\,b$ for a and b exceeding 1 then the first degree polynomial function $f(x) = a \cdot x$ has at least two values that are multiples of n, namely 0 and $f(b)$.

This implies that the polynomial function defined on Int_n by

$$g(x) = [a]_n x$$

has at least two roots: that is, there are at least two different residue classes in Int_n that satisfy the equation $g(x) = [0]_n$.

This is unlike the situation in $\mathbb{R}$ or $\mathbb{C}$ where the number of distinct roots of a polynomial cannot exceed the degree of the polynomial.

However if n is *prime* we do recover this useful fact.

Note that if n is prime then Int_n is a field so if g is any nonzero polynomial we can multiply g by the multiplicative inverse of its leading coefficient to produce a polynomial with exactly the same roots but which has leading coefficient $[1]_n$. Such polynomials are called **monic**. If we can prove the result for monic polynomials of a certain degree we will have it, thereby, for any polynomial of that degree.

11.2. ***Theorem. Lagrange's***[14] ***Theorem:***
Suppose p is prime and that polynomial $g(x)$ with coefficients in Int_p has degree $d > 0$. Then g has at most d distinct roots in Int_p.

Proof. The result is obviously true when polynomial g has degree 1. Assume we have the result for all polynomials of degree less than some degree d and that g is monic with degree d and has (at least) d distinct roots $r_1, r_2, \ldots, r_d$ in Int_p. Then the polynomial

$$g(x) - (x - r_1)\,(x - r_2) \cdots (x - r_d)$$

has degree lower than d but has d distinct roots. So it is the zero polynomial: that is, $g(x) = (x - r_1)\,(x - r_2) \cdots (x - r_d)$. But then if c is any member of Int_p not among the r_i all of the factors $c - r_i$ are nonzero and hence the product of all of them is nonzero. So g cannot have any roots but those already enumerated: g has exactly d roots.

We conclude, invoking Finite Induction (II), that no polynomial of this type has more distinct roots than its degree. □

11.3. **Remark**. If f is a polynomial with coefficients in $\mathbb{Z}$ we can create a polynomial on Int_n via

$$f(x) = a_d x^d + \cdots + a_1 x + a_0 \longleftrightarrow g(X) = [a_d]_n X^d + \cdots + [a_1]_n X + [a_0]_n.$$

Any of the coefficients of f which are multiples of n are zero in Int_n so the degree of g may be lower than the degree of f.

[14] Joseph-Louis Lagrange 1736-1813

11.4. ***Corollary.*** *Suppose p is prime and that polynomial $f(x)$ with coefficients in $\mathbb{Z}$ has degree $d > 0$. Unless* ***all*** *coefficients of f are multiples of p the value of f is a multiple of p for integers in at most d distinct p-congruency classes.*

Now on to a different matter.

It may happen that $o_n(a) = \phi(n)$ and if so every member of $RelPrime_n$ is some power of $[a]_n$. In this case a is called a **primitive root** mod n.

11.5. ***Theorem.*** *If p is prime there is a primitive root mod p. In fact, there are exactly $\phi(c)$ elements of order c in Int_p for every positive factor c of $\phi(p) = p - 1$.*

Proof. We know by Gauss' Theorem that $p - 1 = \sum_{c|(p-1)} \phi(c)$.

Let $\Psi(c)$ be the number of members of Int_p of order c. We know $\Psi(c)$ is nonzero only for divisors of $p - 1$, and every member of Int_p is counted in one $\Psi(c)$.

So we have shown

$$p - 1 = \sum_{c|(p-1)} \Psi(c) = \sum_{c|(p-1)} \phi(c).$$

We will show that corresponding terms in the sums are equal, which yields the statement of the theorem.

We do this by showing that $\Psi(c) \leq \phi(c)$ for every divisor c of $p - 1$.

It is obvious that $\Psi(c) \leq \phi(c)$ whenever $\Psi(c) = 0$.

And if $\Psi(c) \neq 0$ then there is an element $[a]_p$ of order c.

$$[a]_p,\ [a]_p^2,\ \ldots,\ [a]_p^c = [1]_p$$

provides a list of c distinct solutions to the equation

$$x^c = [1]_p.$$

By Lagrange's Theorem there can be no more solutions so this list contains *all* members of Int_p whose order divides c. There are $\phi(c)$ of these powers of $[a]_p$ whose orders are not just divisors of c but *exactly* c.

The desired conclusion follows. □

11.6. **Remark**. Note that if t is a primitive root mod p then

$$(t^k)^{\frac{p-1}{2}} \equiv 1 \text{ or } -1 \mod p \quad \text{depending on if } k \text{ is even or odd.}$$

In particular, we have $t^{\frac{p-1}{2}} \equiv -1 \mod p$.

12. **Wilson's Theorem.**

Suppose p is prime.

Lagrange's Theorem implies that the only value(s) of x for which

$$x^2 \equiv 1 \mod p$$

are of the form $x = 1 + t \cdot p$ and $x = -1 + t \cdot p$ for arbitrary integers t. (These classes of solutions are equivalent if $p = 2$.)

So in Int_p the only solutions to $X^2 = [1]_p$ are

$$X = [1]_p \quad \text{and} \quad X = [-1]_p = [p-1]_p.$$

The other nonzero members of the field Int_p can be organized into distinct multiplicative-inverse pairs which means that

$$(p-1)! = 1(p-1) \cdot (1 + \text{a multiple of } p).$$

So $(p-1)! \equiv -1 \mod p$.

On the other hand if some number n is exceeds 1 but is not prime then it can be factored into two smaller unequal positive integers or $n = k^2$ for some k exceeding 1.

In the first case, if $n = ab$ for unequal a and b then both a and b are among the factors of $(n-1)!$ so $(n-1)! \equiv 0 \mod n$.

In the second case, such as $n = 2^2 = 4$, we have $3! = 6 = 2 \mod 4$.

More generally, if $n = k^2$ for k exceeding 2 then both $2k$ and k are among the list of factors of $(n-1)!$ so, again, we have $(n-1)! \equiv 0 \mod n$.

These facts, assembled, yield:

12.1. ***Theorem. Wilson's Theorem***[15]***:***
Integer $n \geq 2$ is prime if and only if $(n-1)! \equiv -1 \mod n$.

12.2. **Remark**. An alternative proof can be created using Fermat's Little Theorem, Lagrange's Theorem and the polynomials

$$f(x) = (x-1)(x-2)\cdots(x-(p-1)) \quad \text{and} \quad g(x) = x^{p-1} - 1.$$

For prime p exceeding 2 every nonzero member of Int_p is a root of *both* equations (after you replace all coefficients by their p-congruency classes) but the difference of these two polynomials is degree $p-2$ and therefore by Lagrange's Theorem must be the zero polynomial. So the constant terms of these two polynomials coincide.

Though an interesting result for other reasons, direct use of Wilson's Theorem as a "prime detector" is computationally tractable only when it is unnecessary.

[15]This theorem was stated as true by Ibn al-Haytham 965-1040 AD around 1000 AD and again, about 750 years later, by John Wilson 1741-1793. Lagrange gave the first actual proof in 1771.

13. **Polynomial Congruencies: Reduction to Simpler Form.**

13.1. **Remark**. We produced, in Section 6.1, conditions for solution of Diophantine equations $ax + my = c$ which, when transformed into modular arithmetic, corresponds to solutions to the first degree polynomial equation

$$ax - c \equiv 0 \mod m.$$

We found that there will be a solution exactly when $d = gcd(a, m)$ divides c, and enumerated the d distinct mod m classes of solutions when a solution exists. If x_0 is any solution all others are of the form

$$x_i = x_0 + i \cdot \frac{m}{d}$$

and these solutions are all in one of the (distinct) conjugacy classes

$$\left[x_0 + i \cdot \frac{m}{d}\right]_m \qquad \text{for } i = 0, \ldots, d-1.$$

These congruence classes correspond to the solutions in Int_m of the first degree equation

$$[a]_m \cdot X = [c]_m.$$

We also learned how to solve *systems* of first degree congruencies in Section 9, the Chinese Remainder Theorem.

The next step is to solve quadratic and higher-degree congruencies and equations.

Suppose f is any polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$. For integer $m \geq 2$ let $g(X)$ be the associated polynomial with coefficients in Int_m given by $g(X) = [a_n]_m X^n + \cdots + [a_1]_m X + [a_0]_m$.

Of course the degree of g might be less than n since $[a_n]_m$ could be $[0]_m$.

So we seek solutions to the **polynomial congruency** or (completely equivalently) solutions to the polynomial equation in Int_m given by

$$f(x) \equiv 0 \mod m \qquad \Longleftrightarrow \qquad g(X) = [0]_m.$$

This is a generalization of an important case, the **general quadratic congruency**

$$\alpha x^2 + \beta x + \gamma \equiv 0 \mod m \quad \Longleftrightarrow \quad [\alpha]_m X^2 + [\beta]_m X + [\gamma]_m = [0]_m.$$

13.2. **Remark**. Suppose $m = s \cdot t$ where $gcd(s, t) = 1$ and, somehow, we find integers x_1 and x_2 for which

$$f(x_1) \equiv 0 \mod s \quad \text{and} \quad f(x_2) \equiv 0 \mod t.$$

It is easy to show that any number s-equivalent to x_1 is *also* a solution to the first congruency, and any number t-equivalent to x_2 is a solution to the second congruency.

By the Chinese Remainder Theorem there is a solution x_3 to the simultaneous congruencies

$$x \equiv x_1 \mod s \qquad \text{and} \qquad x \equiv x_2 \mod t$$

and this solution x_3 is mod $s \cdot t = m$ unique.

So $x_3 + j \cdot m$ for various integers j are all, and the only, solutions to the simultaneous congruencies above.

And conversely any solution to $f(x) \equiv 0 \mod m$ must satisfy the two simultaneous congruencies.

An easy extension of this argument implies that if $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_j^{k_j}$ is the prime factorization of m into the product of distinct prime powers then any solution to

$$f(x) \equiv 0 \mod m$$

will *also* be a solution to each

$$f(x) \equiv 0 \mod p_i^{k_i}.$$

And *if* we can find solutions to all of the the prime-power congruencies we can use the Chinese Remainder Theorem to find all solutions to $f(x) \equiv 0 \mod m$ that correspond to (the prime power classes of) the selected solutions to the individual congruencies, and the Chinese Remainder Theorem guarantees that the solution is unique mod m.

Of course if there is more than one prime power class of solutions for a given prime power modulus, as there likely will be in many cases, we will have to look at all possible combinations of these classes for various prime powers upon which we will apply the Chinese Remainder Theorem. This may well be tedious, but it does have the virtue of specificity: we will know exactly with which combinations we must work to produce our complete list of solutions and each combination will produce a unique mod m solution to the original equation.

And if any of the prime power congruencies *fails* to have a solution then the original congruency has no solution either.

We enshrine this key fact as a theorem.

13.3. ***Theorem.*** *if $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_j^{k_j}$ is the prime factorization of m into the product of distinct prime powers then every solution of*

$$(i) \qquad f(x) \equiv 0 \mod m$$

is a solution of

$$(ii) \qquad f(x) \equiv 0 \mod p_i^{k_i} \text{ for each } i.$$

Therefore, a necessary condition for the existence of a solution to (i) is that each congruency (ii) have a solution.

Conversely, if each congruency (ii) has a solution then every combination of solutions selected (one for each prime power) can be used to construct a solution to (i) via the Chinese Remainder Theorem.

So it seems we can focus on prime power congruencies in our hunt for solutions to a polynomial congruency.

13.4. **Remark**. Given polynomial $f(x) = a_n x^n + \cdots a_1 x + a_0$ and m as above we select one of the constituent prime powers p^k for m. There are various ways of simplifying the subsequent work.

We can **reduce the coefficients a_i to non-negative values all less than p^k**. We want solutions to

$$f(x) = a_n x^n + \cdots a_1 x + a_0 \equiv 0 \mod p^k$$

and, for convenience, when we mention a **specific solution x we can (if we wish) choose it so that it is non-negative and less than p^k**.

If the a_i share a common factor of p^j so $a_i = p^j \cdot b_i$ for all i and if $j \geq k$ this congruency is trivial: any integer is a solution. But otherwise, the congruency is equivalent to

$$\frac{f(x)}{p^j} = b_n x^n + \cdots + b_1 x + b_0 \equiv 0 \mod p^{k-j}.$$

Therefore we may assume that there is no common p-power factor among the nonzero coefficients. And if the nonzero coefficients share any *other* factor then that factor has a mod p^{k-j} multiplicative inverse so the congruency can be multiplied by that inverse without altering the solution set.

So we may, and do, make the simplifying assumption that if there is more than one non-zero coefficient the greatest common factor of these non-zero coefficients is 1. We will also assume that we really are working with an nth degree polynomial here: that after reduction as above $a_n \neq 0$.

With these reductions we have arrived at a mod p^k congruency and where

$$f(x) = x^n \qquad \text{or} \qquad f(x) = p^j x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

The first case is trivial to solve and in the second case $0 \leq j < k$ and there is at least one non-zero term among the coefficients $a_0, \ldots, a_{n-1}$ and at least one of these does *not* have a factor of p.

14. **Polynomial Congruencies: Solutions.**

14.1. **Remark**. Recall that any polynomial can be expanded in a finite power series around any point, and in our case we can produce the representation

$$\begin{aligned} f(x+u) &= f(x) + \frac{f'(x)}{1!}u + \left(\frac{f''(x)}{2}u^2 + \cdots + \frac{f^{(n)}(x)}{n!}u^n\right) \\ &= f(x) + f'(x)\cdot u + u^2\left(\frac{f''(x)}{2} + \cdots + \frac{f^{(n)}(x)}{n!}u^{n-2}\right). \end{aligned}$$

The kth derivatives $f^{(k)}(x)$ in this formula are terms of the form

$$j\cdot(j-1)\cdots(j-k+1)\cdot a_j\cdot x^{j-k+1}$$

and in view of Proposition 3.3 the ratios $\frac{j\cdot(j-1)\cdots(j-k+1)}{k!}$ are all integers. Therefore the parenthesized term in the last line of the power series representation of $f(x+u)$ is an integer, which is then multiplied by u^2.

We note for later that if g is any polynomial and $p|g(x)$ for some x then $p|g(x+v\cdot p)$ for any integer v. Therefore, for each x all or none of the numbers $g(x+v\cdot p)$ are divisible by p.

Now suppose we have polynomial f and $k\geq 2$. Examining the power series, if $0<v<p$ we have

$$f(x+v\cdot p^{k-1}) = f(x) + f'(x)\cdot v\cdot p^{k-1} + v^2\cdot p^{2k-2}M(v)$$

for an integer $M(v)$ depending on x and v. Observe $2k-2\geq k$.

When finding solutions, it will be useful to note that if $f(x)\not\equiv 0 \mod p^k$ but $p|f'(x)$ then $f(x+v\cdot p^{k-1})\not\equiv 0 \mod p^k$ for any v with $0\leq v<p$. In other words if x is not a mod p^k solution and $p|f'(x)$ then $x+v\cdot p^{k-1}$ cannot be mod p^k solutions either for any of these v.

On the other hand if $p\nmid f'(x)$ and assuming only that x is a mod p^{k-1} solution then there can be at most one mod p^k solution among the numbers $x+v\cdot p^{k-1}$ for $v=0,\ldots,p-1$, as can be seen by examining a difference

$$f(x+v\cdot p^{k-1}) - f(x+w\cdot p^{k-1}).$$

Now suppose we have solution x_0 to $f(x)\equiv 0 \mod p^k$. So $f(x_0)=c\cdot p^k$ for some c and we can choose x_0 itself so that $0\leq x_0<p^k$, and we will make that mod p^k equivalent choice.

Then for some v with $0\leq v<p$ we have $0\leq x_0 - v\cdot p^{k-1}<p^{k-1}$ and the number $x_1 = x_0 - v\cdot p^{k-1}$ is among the solutions to $f(x)\equiv 0 \mod p^{k-1}$.

With this setup in hand, we have

$$f(x_0) = f(x_1 + v\cdot p^{k-1}) = f(x_1) + f'(x_1)\cdot v\cdot p^{k-1} + p^k N$$

for an integer N.

So if $p|f'(x_1)$ the number x_1 must *also* be a solution to $f(x) \equiv 0 \mod p^k$, and it follows that $x_1 + v \cdot p^{k-1}$ is a solution not only for the specified value of v but for *any* value of v, and these various possible v values (include $v = 0$ here) provide a total of p distinct mod p^k solutions to $f(x) \equiv 0 \mod p^k$. They are, of course, different versions of the *same* mod p^{k-1} solution but the p^k modulus is able to distinguish them.

But if $p \nmid f'(x_1)$ for some known p^{k-1} solution x_1 (we don't know x_0 here—we want to find it) then at most one of the numbers on the list

$$x_1, \quad x_1 + p^{k-1}, \quad x_1 + 2 \cdot p^{k-1}, \quad , \ldots , \quad x_1 + (p-1) \cdot p^{k-1}$$

could be a p^k solution. And the v that corresponds to this potential solution, if it exists, must satisfy

$$-f'(x_1) \cdot v \equiv \frac{f(x_1)}{p^{k-1}} \mod p.$$

Under these conditions a unique v with $0 \leq v < p - 1$ that satisfies this congruency can be found. However it still must be verified for this calculated v that the assumption that *produced* the congruency, namely that there *is* a value of v for which $x_1 + v \cdot p^{k-1}$ is a mod p^k solution, is valid.

14.2. **Remark**. So we now have a method for finding all the solutions to

$$f(x) = p^j x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \mod p^k$$

by "working up" from lower p-power congruencies, *assuming we can find all solutions to at least one of these.*

If there are s solutions to a lower mod p^i congruency the method we outline below requires the evaluation of $f(x)$ and $f'(x)$ on each solution. It *could* (but often won't) produce as many as $s \cdot p$ different mod p^{i+1} solutions. The total number of necessary evaluations, moving up from the mod p^i solutions to the mod p^k solutions, will usually be far fewer than the worst-case of p^k evaluations which would be required by selecting a representative from each of the classes in Int_{p^k} to find all mod p^k solutions directly. As we have seen in Corollary 11.4, the number of mod p solutions (the typical starting case of $i = 1$) cannot exceed n unless p divides all coefficients, a situation we forbid by preliminary reduction.

If $j \geq i > 0$ the leading term is congruent to 0 mod p^i, so the polynomial is actually of lower degree and under our conditions it is *not* the zero polynomial.

Generally, you can replace the polynomial congruence with one that is equivalent for that p-power. For instance if you are starting at level $i = 1$ for $p = 7$ an expression like $x^8 + 9x + 8 \equiv 0 \mod 7$ could be replaced[16] (Fermat's Little Theorem) by $x + 9x + 1 \equiv 3x + 1 \equiv 0 \mod 7$. Remember

[16]Technically speaking, $x^8 + 9x + 8$ and $3x + 1$ are not equivalent mod 7 *as polynomials* which, by definition, must have terms of identical degree and congruent corresponding

though, as you move up the p-power congruencies, to replace reductions with those appropriate to that p-power from the *original* polynomial.

You may choose judiciously where to start this procedure though $i = j$ or $i = 1$ may be good choices. Choosing the starting i value to be larger is better *if you can solve the resulting polynomial congruency.*

If at any point in the following description we arrive at a congruency with no solution the the original congruency has no solution.

We proceed as follows. Suppose k is at least 2.

Find all solutions, if you can, for the congruency $f(x) = p^j x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \mod p^i$ for some i with $0 < i < k$.

Each mod p^{i+1} solution, if any, will be p^{i+1} equivalent to one of the numbers $x + v \cdot p^i$ for some $v = 0, \ldots, p-1$ and some mod p^i solution x.

Suppose x is among these mod p^i solutions, chosen so that $0 \leq x < p^i$.

If $p^{i+1} | f(x)$ check to see if $p | f'(x)$ and if it does every number of the form $x + v \cdot p^i$ for $v = 1, \ldots, p-1$ is *also* a mod p^{i+1} solution. Include them all.

If $p^{i+1} \nmid f(x)$ but $p | f'(x)$ the numbers $x + v \cdot p^i$ are *not* mod p^{i+1} solutions. Rule them all out.

If $p^{i+1} | f(x)$ but $p \nmid f'(x)$ the numbers $x + v \cdot p^i$ are *not* mod p^{i+1} solutions unless $v = 0$. Include x in the list of mod p^{i+1} solutions, rule the others out.

If $p^{i+1} \nmid f(x)$ and $p \nmid f'(x)$ solve the congruency

$$-f'(x) \cdot v \equiv \frac{f(x)}{p^i} \mod p$$

for v with $0 < v < p$. There will be just one value of v under our conditions, and this calculated value will provide the only *possible* mod p^{i+1} solution of the form $x + v \cdot p^i$, but it must be determined if p^{i+1} actually does divide $f(x + v \cdot p^i)$. Include it or not depending on this.

Proceed through the list of mod p^i solutions until each has been ruled out, included alone, used to find a single v for which $x + v \cdot p^i$ is a mod p^{i+1} solution or included and expanded into p different numbers which are p^i equivalent but which are distinct mod p^{i+1} solutions.

Finally, proceed for g steps, until $i + g = k$.

14.3. **Remark**. We give some examples of these methods in action, following the treatment in *An Introduction to the Theory of Numbers* [NZ62] by Niven and Zuckerman.

$$\textbf{Solve} \qquad \boldsymbol{x^2 + x + 7 \equiv 0 \mod 3^3.}$$

$f(x) = x^2 + x + 7 \equiv 0 \mod 3$ has the single solution 1 by inspection.

---

coefficients. However they produce mod 7 equivalent *output* when evaluated at any integer, which is what we care about here.

$f(1) = 9$ and $f'(x) = 2x + 1$ and $3|f'(1)$ so 1 and 4 and 7 are all solutions to $x^2 + x + 7 \equiv 0 \mod 9$.

$27 \nmid f(1) = 9$ but $3|f'(1)$ so $1, 10$ and 19 are ruled out as mod 27 solutions.

$27|f(4) = 27$ and $3|f'(4) = 9$ so $4, 13$ and 22 are all mod 27 solutions.

$27 \nmid f(7) = 63$ and $3|f'(7) = 15$ so $7, 16$ and 25 are ruled out as mod 27 solutions.

So the mod 27 classes of $4, 13$ and 22 are the solutions.

Solve $\quad x^2 + x + 7 \equiv 0 \mod 3^4$.

$81 \nmid f(4) = 27$ and $3|f'(4)$ so none of $4, 31$ or 58 are mod 81 solutions.

$81 \nmid f(13) = 189$ and $3|f'(13)$ so none of $13, 40$ or 67 are mod 81 solutions.

$81 \nmid f(22) = 513$ and $3|f'(22)$ so none of $22, 49$ or 76 are mod 81 solutions.

So there are no solutions to this congruency.[17]

Solve $\quad x^2 + x + 7 \equiv 0 \mod 7^3$. $\quad -56, 55$

0 and 6 are the only mod 7 solutions, by inspection. $f'(x) = 2x + 1$.

$7 \nmid f'(0) = 1$ and $49 \nmid f(0)$. Solve $-1 \cdot v \equiv 1 \mod 7$.

This gives $v = 6$ so $0 + 6 * 7 = 42$ is a mod 49 solution.

$7 \nmid f'(6) = 18$ and $49|f(6) = 49$. So 6 is a mod 49 solution.

$7^3 = 343 \nmid f(42) = 1813$ and $7 \nmid f'(42) = 85$.

For $x = 42$ solve $1813/49 = 37 \equiv -85 \cdot v \mod 7$.

This is equivalent to $2 \equiv 6 \cdot v \mod 7$.

So $v = 5$ and the mod 7^3 solution is $42 + 5 * 49 = 287$.

For $x = 6$ solve $49/49 = 1 \equiv -13 \cdot v \mod 7$.

This is equivalent to $1 \equiv 1 \cdot v \mod 7$ which has solution $v = 1$.

So $6 + 1 \cdot 49 = 55$ is a mod 7^3 solution.

So the mod 7^3 classes of 287 and 55 are the solutions.

Solve $\quad x^5 + x^4 + 1 \equiv 0 \mod 3^4$.

1 is the only mod 3 solution, by inspection. $f'(x) = 5x^4 + 4x^3$.

$9 \nmid f(1) = 3$ and $3|f'(1) = 9$.

There are no mod 3^2 solutions so there are no mod 3^4 solutions.

[17] We used the fact that $3|f'(4)$, determined in the previous example. We know then that $3|f'(13)$ and $3|f'(22)$ since both 13 and 22 differ from 4 by a multiple of 3.

Solve $\quad 25x^3 + x + 57 \equiv 0 \mod 5^3.$

Starting with mod 25 this is $x + 7 \equiv 0 \mod 25$ with solution $x = 18$.

$f'(x) = 75x^2 + 1$ and $5 \nmid f'(18) = 24301$.

$125 | f(18) = 145875$ so the class of 18 is the only mod 125 solution.

Solve $\quad x^2 + 5x + 24 \equiv 0 \mod 36.$

We need to solve

$x^2+5x+24 \equiv x^2+5x+6 \equiv 0 \mod 9$ and $x^2+5x+24 \equiv x^2+x \equiv 0 \mod 4$

and apply the Chinese Remainder Theorem to the solution combinations.

The first congruency has solutions $6, 7$ and the other has solutions $0, 3$.

Note $9(1) + 4(-2) = 1$ so, for instance, $9(1) = 1 - 4(-2)$.

The simultaneously congruent solutions will be mod 36 congruent to

$$a_1 \cdot 4 \cdot (-2) + a_2 \cdot 9 \cdot (1)$$

where a_1 is a solution to the mod 9 congruency and a_2 is a solution to the mod 4 congruency.

$6 \cdot 4 \cdot (-2) + 0 \cdot 9 \cdot (1) = -48 \equiv 24 \mod 36$

$6 \cdot 4 \cdot (-2) + 3 \cdot 9 \cdot (1) = -21 \equiv 15 \mod 36$

$7 \cdot 4 \cdot (-2) + 0 \cdot 9 \cdot (1) = -56 \equiv 16 \mod 36$

$7 \cdot 4 \cdot (-2) + 3 \cdot 9 \cdot (1) = -29 \equiv 7 \mod 36$

So the mod 36 classes of $7, 15, 16$ and 24 are the solutions.

15. The Quadratic Formula.

To solve a general real quadratic equation one uses the **quadratic formula**, and the key step in that solution is the possibility of evaluating the square root in the formula.

A general quadratic mod m congruency has the form

$$\alpha x^2 + \beta x + \gamma \equiv 0 \mod m.$$

But now we will make a specific restriction.

We will presume in this section that $m \nmid 4 \cdot \alpha$.

In view of the result of Theorem 13.3 the case of $m = p^k$ is of primary interest to us.

Multiplying the quadratic equation by 4α produces

$$4\alpha^2 x^2 + 4\alpha\beta x + 4\alpha\gamma \equiv 0 \mod m.$$

and adding $\beta^2 - \beta^2$ we have

$$4\alpha^2x^2 + 4\alpha\beta x + \beta^2 + 4\alpha\gamma - \beta^2 \equiv 0 \mod m$$

and then

$$(\,2\alpha x + \beta\,)^2 \equiv \beta^2 - 4\alpha\gamma \mod m.$$

So we can turn this equation into a linear equation and attempt to solve that provided we have a way to find all mod m square roots of $A = \beta^2 - 4\alpha\gamma$.

If we *cannot* find square roots of A then, under our conditions, there will be no solution to the quadratic congruency.

Further, given success there, we are *guaranteed* to find solutions (using our ruminations about solutions of Diophantine equations) when and only when

$$d = gcd(2\alpha, m) \mid \sqrt{A} - \beta$$

and for each $\sqrt{A}$ for which this condition holds there will be d distinct mod m solutions to the original quadratic.

If in fact $d = 1$ we have at most one solution for each $\sqrt{A}$.

So it seems we must consider square roots for various moduli. Some data for specific small moduli might be a place to start, as found in the nearby table.

Of course 0 and 1 always are their own square roots, and the numbers which *have* square roots, listed in the columns in the table, are symmetric, due to the fact that if a has a square root x for modulus m then $m - x$ is a second square root for that modulus.

We take up the issue of square roots (and their existence) in more detail in subsequent sections.

16. **Square Roots for Prime Power Moduli.**

16.1. ***Lemma.*** *Suppose p is an odd prime and $gcd(a, p) = 1$.*
Suppose also $k > j \geq 1$ and we have found a solution for $x^2 \equiv a \mod p^j$.
This solution can be used to find an explicit solution to $x^2 \equiv a \mod p^k$.

Proof. Suppose $x^2 \equiv a \mod p^j$ for some $j \geq 1$. So $x^2 = a + c \cdot p^j$ for some integer c. It may be that $p|c$ in which case $x^2 \equiv a \mod p^{j+1}$.

But if not, since x can have no factor of p there is a number y so that $2xy \equiv -c \mod p$. Thus $2xy = -c + z \cdot p$ for some integer z.

Now Let $w = x + y \cdot p^j$.

$$\begin{aligned} w^2 = \left(x + y \cdot p^i\right)^2 &= x^2 + 2xyp^j + y^2p^{2j} \\ &= a + c \cdot p^j + (-c + z \cdot p)p^i + y^2p^{2j} = a + \left(x + y^2p^{j-1}\right)p^{i+1}. \end{aligned}$$

So $w^2 \equiv a \mod p^{j+1}$.

modulus

	3	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
$\mathbf{1^2} = 1$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\mathbf{2^2} = 4$	1	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
$\mathbf{3^2} = 9$		1	4	3	2	1	0	9	9	9	9	9	9	9	9	9	9
$\mathbf{4^2} = 16$			1	4	2	0	7	6	5	4	3	2	1	0	16	16	16
$\mathbf{5^2} = 25$				1	4	1	7	5	3	1	12	11	10	9	8	7	6
$\mathbf{6^2} = 36$					1	4	0	6	3	0	10	8	6	4	2	0	17
$\mathbf{7^2} = 49$						1	4	9	5	1	10	7	4	1	15	13	11
$\mathbf{8^2} = 64$							1	4	9	4	12	8	4	0	13	10	7
$\mathbf{9^2} = 81$								1	4	9	3	11	6	1	13	9	5
$\mathbf{10^2} = 100$									1	4	9	2	10	4	15	10	5
$\mathbf{11^2} = 121$										1	4	9	1	9	2	13	7
$\mathbf{12^2} = 144$											1	4	9	0	8	0	11
$\mathbf{13^2} = 169$												1	4	9	16	7	17
$\mathbf{14^2} = 196$													1	4	9	16	6
$\mathbf{15^2} = 225$														1	4	9	16
$\mathbf{16^2} = 256$															1	4	9
$\mathbf{17^2} = 289$																1	4
$\mathbf{18^2} = 324$																	1

So either x is *already* a mod p^{j+1} square root of a, or it can be used to produce one.

We continue this process up to exponent k and the result is proved. □

16.2. **Remark**. Square roots for both members of Int_2 exist, an uninteresting case.

In Int_4 we have

$$[1]_4^2 = [1]_4 \text{ and } [3]_4^2 = [9]_4 = [1]_4.$$

So if a is coprime to 4 then a has a mod 4 square root exactly when $a \equiv 1$ mod 4. Both members of $RelPrime_4$ are square roots of $[1]_4$. Of course $[0]_4^2 = [2]_4^2 = [0]_4$ so $[0]_4$ also has two square roots.

$$0^2 = 0 \quad \text{and} \quad 1^2 = 1 \quad \text{and} \quad 2^2 = 4 \quad \text{and} \quad 3^2 = 9 = 1 + 8$$
$$\text{and} \quad 4^2 = 16 = 2 * 8 \quad \text{and} \quad 5^2 = 25 = 1 + 3 \cdot 8$$
$$\text{and} \quad 6^2 = 36 = 4 + 4 * 8 \quad \text{and} \quad 7^2 = 49 = 1 + 6 \cdot 8.$$

So in $RelPrime_8$ only $[1]_8$ has a square root, and all four elements of $RelPrime_8$ are square roots of $[1]_8$. The classes $[3]_8$, $[5]_8$ and $[7]_8$ have no square roots.

Among the rest of the members of Int_8 only the classes $[0]_8$ (roots $[0]_8$ and $[4]_8$) and $[4]_8$ (roots $[2]_8$ and $[6]_8$) have square roots. $[2]_8$ and $[6]_8$ have no square roots.

16.3. ***Lemma.*** *Suppose a is odd.*

(i) $x^2 \equiv a \mod 2$ always has a solution: every member of $[1]_2$.

(ii) $x^2 \equiv a \mod 4$ has a solution only when $a \equiv 1 \mod 4$.

(iii) $x^2 \equiv a \mod 2^k$ for $k \geq 3$ has a solution exactly when $a \equiv 1 \mod 8$.

In the proof of (iii) we show how to calculate, from a solution to $x^2 \equiv a \mod 2^3$, an explicit solution to $x^2 \equiv a \mod 2^k$ when $k > 3$.

Proof. We demonstrated the lemma to be true (see the table) up to modulus $2^4 = 16$ by examining all cases.

Suppose $x^2 \equiv a \mod 2^k$ for some $k \geq 3$. Since a is odd so too is x, which must therefore be of the form $x = 1 + 2 \cdot r$. But then

$$x^2 = 1 + 4r + 4r^2 = 1 + 4r(1 + r)$$

and whether r is even or odd the term $4r(1 + r)$ is divisible by 8. So it is *necessary* that $a \equiv 1 \mod 8$ for a square root to exist.

Suppose we know that for a specific k, at least three, that $x^2 \equiv a \mod 2^k$ whenever $a \equiv 1 \mod 8$ and suppose a is such a number with mod 2^k square root x.

Thus $x^2 = a + r \cdot 2^k$ for some integer k.

If r is even, then x is also a mod 2^{k+1} square root of a.

But r may be odd. In that case, since both x and a are odd there exists y for which $xy = -r + 2j$. So now

$$\begin{aligned}\left(x + y \cdot 2^{k-1}\right)^2 &= x^2 + 2 \cdot x \cdot y \cdot 2^{k-1} + y^2\, 2^{2(k-1)} \\ &= a + r \cdot 2^k + 2 \cdot (-r + 2j) \cdot 2^{k-1} + y^2\, 2^{2(k-1)} \\ &= a + j \cdot 2^{k+1} + y^2\, 2^{2(k-1)} \equiv a \mod 2^{k+1}.\end{aligned}$$

So either the mod 2^k square root x is *already* a mod 2^{k+1} square root of a, or it can be used to produce one which, it should be noted, is also a *different* mod 2^k square root of a.

The result now follows by induction on the exponent on the modulus. □

16.4. ***Theorem.*** *Suppose $a = 2^j \cdot \alpha$ where α is odd and $j \geq 0$.*

(i) $x^2 \equiv a \mod 2$ always has a solution.

If $j > 0$ the solution set is $[0]_2$. If $j = 0$ the solution set is $[1]_2$.

(ii) $x^2 \equiv a \mod 4$ has a solution exactly when (j is at least 2) or ($j = 0$ and $\alpha \equiv 1 \mod 4$).

(iii) $x^2 \equiv a \mod 2^k$ for $k \geq 3$ has a solution exactly when ($j \geq k$) or (j is even and $x^2 \equiv \alpha \mod 2^{k-j}$ has a solution.),

17. Euler's Criterion and the Legendre Symbol.

17.1. **Remark**. We identify below a condition, found by Euler, under which

$$x^2 \equiv a \mod p \iff Y^2 = [a]_p \qquad (Y = [x]_p)$$

will have solutions for prime p.

The a for which these solutions exist are called **quadratic (or p-quadratic) residues**. The other integers are called **quadratic non-residues**.

The proof of the following result is trivial, but the result itself is important.

17.2. ***Lemma.*** *Suppose p is prime and a, b are p-quadratic residues. So are ab and a^{-1} and $a + np$ for any n.*

17.3. **Remark**. When $p = 2$ the situation is trivial, so we concentrate on odd primes.

The **Legendre**[18] **Symbol** is traditionally employed in this discussion, and we define it for odd prime p (pronounced "a on p") by

$$\left(\frac{\boldsymbol{a}}{\boldsymbol{p}}\right) = \begin{cases} 1 & \text{if } a \text{ is a } p\text{-quadratic residue and } a \not\equiv 0 \mod p \\ 0 & \text{if } a \equiv 0 \mod p \\ -1 & \text{if } a \text{ is a } p\text{-quadratic non-residue.} \end{cases}$$

$a = 0$ is certainly a p-quadratic residue and also j^2 for $j = 1, 2, \ldots, \frac{p-1}{2}$.

If $1 \leq j < k \leq \frac{p-1}{2}$ then $k^2 - j^2 = (k-j)(j+k)$ and both factors are less than prime p so these two squares are not congruent quadratic residues.

Therefore there are *at least* $\frac{p-1}{2}$ distinct nonzero classes of quadratic residues in Int_p.

By Fermat's Little Theorem if $[a]_p \neq [0]_p$ we have

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p.$$

But if a is congruent to x^2 then the left factor is congruent to 0 and the right factor is *not*. This means that there can be *at most* $\frac{p-1}{2}$ distinct nonzero classes of quadratic residues in Int_p, and therefore *exactly* that many.

All the remaining nonzero classes, the classes of quadratic non-residues, correspond to integers that make the second factor a multiple of p. For these classes $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

In any event, we have the following criterion for quadratic residue status.

[18] Adrien-Marie Legendre 1752-1833

17.4. ***Theorem. Euler's Criterion:***

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \qquad \textit{(for odd prime } p\textit{).}$$

a is a p-quadratic residue depending on whether $a^{\frac{p-1}{2}} \equiv 1 \mod p$, in which case it is, or $a^{\frac{p-1}{2}} \equiv -1 \mod p$, in which case it's not, or $a^{\frac{p-1}{2}} \equiv 0 \mod p$, in which case it is, trivially. The three cases exhaust all possibilities.

17.5. ***Corollary.*** *Suppose p is an odd prime and b, c are integers.*

$$\textit{Then} \quad \left(\frac{b\cdot c}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right) \quad \textit{and} \quad \left(\frac{b+np}{p}\right) = \left(\frac{b}{p}\right) \textit{for any } n.$$

17.6. ***Corollary.*** *Suppose p is an odd prime and a is any integer. Then*

$$a = (-1)^i \cdot 2^j \cdot p_1 \dots p_k \cdot p^m \cdot N^2$$

for primes $p_1, \dots, p_k$ not p or 2 and i, j are 0 or 1 and $p \nmid N$.

$$\textit{Then} \quad \left(\frac{a}{p}\right) = \left(\frac{(-1)^i}{p}\right)\left(\frac{2^j}{p}\right)\left(\frac{p^m}{p}\right)\left(\frac{p_1}{p}\right)\cdots\left(\frac{p_k}{p}\right).$$

17.7. **Remark**. In Corollary 17.6 the case where $m \neq 0$ is trivial, so we can reduce the problem of calculating a general $\left(\frac{a}{p}\right)$ to that of finding $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$ for odd primes q less than p.

17.8. **Remark**. We expand a little on the material of Remark 17.3.

If we have a primitive root mod p we can be a bit more explicit about the p-quadratic residues. Suppose t is a primitive root mod p for odd prime p.

The residues of the list $t, t^2, \dots, t^{p-1}$ are exactly the numbers $1, 2, \dots, p-1$ in some order and *half* of the members of the first list, the $\frac{p-1}{2}$ numbers with even exponents, are p-quadratic residues. The odd exponent terms are the quadratic non-residues.

Generally if $x^2 \equiv y^2 \mod p$ and $x \neq 0 \mod p$ then $x \equiv \pm y \mod p$.

So there are three possibilities for solutions to $x^2 \equiv a \mod p$.

First $x \equiv 0 \mod p$. Second, $p = 2$ and there is just one solution, $1 \equiv -1 \mod 2$. Third, there are exactly two congruence classes of solutions and if r is a residue of one solution $p - r$ is the residue of the second. On of these residues is no more than $\frac{p-1}{2}$ while the other is, at least, $\frac{p+1}{2}$.

As an example, assuming p to be odd, since $\left(t^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p$ and $t^{\frac{p-1}{2}} \not\equiv 1 \mod p$ it must be that $t^{\frac{p-1}{2}} \equiv -1 \mod p$.

Any $a \equiv t^k \mod p$ for some k and then $a^{\frac{p-1}{2}} \equiv t^{k\,\frac{p-1}{2}}$. If k is even a is a p-quadratic residue and $a^{\frac{p-1}{2}} \equiv 1 \mod p$. But if k is odd a is a p-quadratic non-residue and $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

This is an alternative argument for Euler's Criterion.

18. **A Lemma of Gauss.**

Again we presume p is an odd prime and this time assume a to be relatively prime to p.

Examine the list of $\frac{p-1}{2}$ numbers

$$a,\ 2\cdot a,\ 3\cdot a,\ \ldots,\ \frac{p-1}{2}\cdot a.$$

These numbers have nonzero mod p residues and also must have distinct residues.

We index and list these residues in increasing order as

$$0 < r_1 < r_2 < \cdots r_k \le \frac{p-1}{2} < \frac{p+1}{2} \le r_{k+1} < \cdots < r_{k+n} < p$$

where, as indicated, k has been chosen to be the index of the greatest residue not exceeding $\frac{p-1}{2}$.

The integer n is the number of these residues which are $\frac{p+1}{2}$ or larger.

$k+n = \frac{p-1}{2}$ so, as far as we know, we could have $n = 0$.

Consider the new list of $\frac{p-1}{2}$ numbers

$$r_1,\ r_2,\ \ldots,\ r_k,\ p-r_{k+1},\ \ldots,\ p-r_{k+n}.$$

which are all bigger than 0 and no larger than $\frac{p-1}{2}$.

We know there there are no repeats among the first k, nor are there any duplicate numbers among the last n.

And if one of the first group is duplicated among the last group, say $r_j = p - r_t$, then for certain positive integers i_1 and i_2 not exceeding $\frac{p-1}{2}$, and for two other integers i_3 and i_4 we would have

$$r_j = p - r_t \quad \longleftrightarrow \quad i_1 a + i_3 p = p - (i_2 a + i_4 p)$$

and therefore $(i_1 + i_2)a = p(1 - i_4 - i_3)$.

This is impossible, in view of the fact that $0 < i_1 + i_2 < p$. So there are no duplicates among these $\frac{p-1}{2}$ positive numbers, none of which exceeds $\frac{p-1}{2}$.

Therefore the numbers $r_1,\ r_2,\ \ldots,\ r_k,\ p-r_{k+1},\ \ldots,\ p-r_{k+n}$ are nothing more than a rearrangement of the numbers from 1 to $\frac{p-1}{2}$.

We now have

$$\begin{aligned} a^{\frac{p-1}{2}}\, 1\cdot 2\cdot 3\cdots\frac{p-1}{2} &= 1\cdot a\cdot 2\cdot a\cdot 3\cdot a\cdots\frac{p-1}{2}\cdot a \\ &\equiv r_1\cdot r_2\cdots r_{k+n} \mod p \\ &\equiv (-1)^n r_1\cdots r_k\cdot(p-r_{k+1})\cdots(p-r_{k+n}) \mod p \\ &\equiv (-1)^n\, 1\cdot 2\cdot 3\cdots\frac{p-1}{2} \mod p \end{aligned}$$

and we conclude that $a^{\frac{p-1}{2}} \equiv (-1)^n \mod p$.

Appealing to Euler's Criterion we have proven a result that would likely be called a theorem if attributed to anyone but Gauss:

18.1. ***Theorem. Gauss' Lemma:***
If p is an odd prime and a is a positive integer with $gcd(a,p)=1$ and n is the number of residues of numbers on the list

$$a,\ 2\cdot a,\ 3\cdot a,\ \ldots,\ \frac{p-1}{2}\cdot a$$

which exceed $\frac{p-1}{2}$ then, in terms of the Legendre symbol,

$$\left(\frac{a}{p}\right) = (-1)^n.$$

In other words, a is a p-quadratic residue or not depending on whether n is even or odd.

Now we prove a technical lemma based on Gauss' Lemma which we will use in our proof of the Quadratic Reciprocity Law, Theorem 20.1.

For integers r, s and t with $t>0$ we say $r \le \frac{s}{t}$ exactly when $r\cdot t \le s$.

For every fraction $\frac{s}{t}$ there is[19] a largest integer r for which $r \le \frac{s}{t}$.

We denote it by the symbols $\left[\frac{s}{t}\right]$, the "**greatest integer in $\frac{s}{t}$**."

18.2. ***Lemma.*** *If n is the number defined in Gauss' Lemma above for **odd** integer a and odd prime p then*

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \mod 2$$

and therefore by Gauss' Lemma

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]}.$$

[19]That there is such an integer for an s,t combination and that it would be the same if calculated using any rational $\frac{a}{b}$ equivalent to $\frac{s}{t}$ requires a little argument.

Proof. Recall the list

$$a,\ 2\cdot a,\ 3\cdot a,\ \ldots,\ \frac{p-1}{2}\cdot a.$$

and their properly ordered mod p residues

$$0 < r_1 < r_2 < \cdots r_k \leq \frac{p-1}{2} < \frac{p+1}{2} \leq r_{k+1} < \cdots < r_{k+n} < p$$

For each j between 1 and $\frac{p-1}{2}$ we have

$$j\cdot a = \left[\frac{ja}{p}\right]\cdot p + r_{i_j}$$

where r_{i_j} is counted among the n "big residues" if it exceeds $\frac{p-1}{2}$.

Adding together all the $j\cdot a$ we have

$$\frac{p^2-1}{8}\cdot a = \sum_{j=1}^{\frac{p-1}{2}} j\cdot a = p\cdot\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] + \sum_{i=1}^{k} r_i + \sum_{i=k+1}^{k+n} r_i.$$

In Gauss' Lemma we showed that the list

$$r_1,\ r_2,\ \ldots\ ,\ r_k,\ p-r_{k+1},\ \ldots\ ,\ p-r_{k+n}$$

is a reordering of the first $\frac{p-1}{2}$ positive integers so

$$\frac{p^2-1}{8} = \left(\sum_{i=1}^{k} r_i\right) + np - \left(\sum_{i=k+1}^{k+n} r_i\right)$$

Subtracting corresponding left and right sides of these equalities produces

$$\frac{p^2-1}{8}\cdot(a-1) = p\cdot\left(-n + \sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]\right) + 2\cdot\sum_{i=k+1}^{k+n} r_i.$$

Since p and a are odd they are both congruent to 1 mod 2, so the line above becomes

$$0 \equiv -n + \sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] \mod 2$$

which is the result we were seeking.

□

19. $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

When is -1 is a p-quadratic residue for odd prime p?

This will happen, according to Euler's Criterion, when and only when $\frac{p-1}{2}$ is even, in which case $p \equiv 1 \mod 4$. Assuming p to be an odd prime the only other possible case is $p \equiv 3 \equiv -1 \mod 4$ and in that case -1 is a p-quadratic non-residue. We have proved:

19.1. ***Lemma.*** *An odd prime p must satisfy $p \equiv 1$ or $3 \mod 4$.*

$$\left(\frac{-1}{p}\right) = 1 \text{ if } p \equiv 1 \mod 4 \quad \text{and} \quad \left(\frac{-1}{p}\right) = -1 \text{ if } p \equiv 3 \mod 4.$$

In terms of a direct formula, Euler's Criterion gives $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

The next lemma involves more cases than we considered in Lemma 19.1.

19.2. ***Lemma.*** *An odd prime p must satisfy $p \equiv 1$ or 3 or 5 or $7 \mod 8$.*

$$\left(\frac{2}{p}\right) = 1 \text{ if } p \equiv 1 \text{ or } 7 \mod 8 \quad \text{and} \quad \left(\frac{2}{p}\right) = -1 \text{ if } p \equiv 3 \text{ or } 5 \mod 8.$$

In terms of a direct formula, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. For odd prime p examine the mod p residues of the numbers

$$2,\ 2\cdot 2,\ 3\cdot 2,\ \ldots,\ \frac{p-1}{2}\cdot 2.$$

None of these numbers equal or exceed p so they *are* their own list of residues, in order. A certain number n of these values will exceed $\frac{p-1}{2}$ and according to Gauss' Lemma $\left(\frac{2}{p}\right) = (-1)^n$. So we need to count how many of these large residues there are for the four possible *mod* 8 residues of our prime p, determining if n is even or odd in each case.

If $p = 1 + 8k$ then $\frac{p-1}{2} = 4k$. The first $2k$ entries on that list (the numbers up to $4k$ after multiplication by 2) do not exceed $4k$. So $\frac{p-1}{2} - 2k = \frac{1+8k-1-4k}{2} = 2k$ are bigger.

If $p = 3 + 8k$ then $\frac{p-1}{2} = 1 + 4k$. The first $2k$ entries on that list (the numbers up to $4k$ after multiplication by 2) do not exceed $1 + 4k$. So $\frac{p-1}{2} - 2k = \frac{3+8k-1-4k}{2} = 2k + 1$ are bigger.

If $p = 5 + 8k$ then $\frac{p-1}{2} = 2 + 4k$. The first $2k + 1$ entries on that list (the numbers up to $4k + 2$ after multiplication by 2) do not exceed $2 + 4k$. So $\frac{p-1}{2} - (2k + 1) = \frac{5+8k-1-4k-2}{2} = 1 + 2k$ are bigger.

If $p = 7 + 8k$ then $\frac{p-1}{2} = 3 + 4k$. The first $2k + 1$ entries on that list (the numbers up to $2 + 4k$ after multiplication by 2) do not exceed $3 + 4k$. So $\frac{p-1}{2} - (2k + 1) = \frac{7+8k-1-4k-2}{2} = 2 + 2k$ are bigger.

This proves the main result. The direct formula is an easy calculation applied to $p = j + 8k$. □

20. **The Law of Quadratic Reciprocity.**

There are reportedly over a hundred distinguishable proofs of the following theorem, six by Gauss alone who created the first complete proof at age 19. The proof given here, appealing to the technical Lemma 18.2, was adapted from one of these, and is due to Ferdinand Eisenstein.

20.1. ***Theorem. The Law of Quadratic Reciprocity***
For distinct odd primes p and q we have

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

That exponent is even unless ***both*** *p and q are congruent to* $3 \mod 4$ *and in that event* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

If ***either*** *is congruent to* $1 \mod 4$ *we have* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Proof. Let R denote the set of points in the plane consisting of all (m, n) for which $1 \le m \le \frac{p-1}{2}$ and $1 \le n \le \frac{q-1}{2}$.

R consists of $\frac{p-1}{2} \cdot \frac{q-1}{2}$ points in a rectangular array in the plane.

None of these points can be on the line $py = qx$ since that would require $p|x$ and none of our points have first coordinate that large.

The points in R above $(i, 0)$ for an allowable i are

$$(i,1)\,,\ \ldots,\ \left(i, \left[\frac{iq}{p}\right]\right),\ \left(i, \left[\frac{iq}{p}\right] + 1\right),\ \ldots,\ \left(i, \frac{q-1}{2}\right)$$

and the first $\left[\frac{iq}{p}\right]$ of these are below the line $py = qx$.

Therefore the number of points in R which are below the line is $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]$.

Similarly, at height i the points in R are

$$(1,\, i)\,,\ \ldots,\ \left(\left[\frac{ip}{q}\right],\ i\right),\ \left(\left[\frac{ip}{q}\right] + 1,\ i\right),\ \ldots,\ \left(\frac{p-1}{2},\ i\right)$$

and the first $\left[\frac{ip}{q}\right]$ of these are to the left of the line $py = qx$ at height i.

So there are $\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right]$ points in R above and to the left of this line.

We have then

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right] + \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]$$

The result now follows immediately from Lemma 18.2.

□

20.2. **Remark**. Let's use the facts we have assembled to calculate whether -59850 is a 29-quadratic residue.

Factoring, we find that $-59850 = (-1)(2)(7)(19)(15^2)$ and $29 \equiv 1 \mod 4$ and $29 \equiv 5 \mod 8$ so

$$\left(\frac{-59850}{29}\right) = \left(\frac{-1}{29}\right)\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)\left(\frac{19}{29}\right) = 1 \cdot (-1) \cdot \left(\frac{7}{29}\right)\left(\frac{19}{29}\right).$$

$\frac{7-1}{2} \cdot \frac{29-1}{2} = 42$, an even number, so

$$\left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

$\frac{19-1}{2} \cdot \frac{29-1}{2} = 126$, also even, so

$$\left(\frac{19}{29}\right) = \left(\frac{29}{19}\right) = \left(\frac{10}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{5}{19}\right) = (-1) \cdot \left(\frac{5}{19}\right)$$

since $19 \equiv 3 \mod 8$. And $\frac{5-1}{2} \cdot \frac{19-1}{2} = 18$ so

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$$

which gives, finally,

$$\left(\frac{-59850}{29}\right) = 1 \cdot (-1) \cdot 1 \cdot (-1) = 1$$

so yes, -59850 is a 29-quadratic residue.

We could approach this another way too. $-59850 \equiv -23 \mod 29$ so

$$\left(\frac{-59850}{29}\right) = \left(\frac{-1}{29}\right) \cdot \left(\frac{23}{29}\right) = \left(\frac{23}{29}\right)$$

since $23 \equiv 1 \mod 4$. And $\frac{23-1}{2} \cdot \frac{29-1}{2}$ is even so

$$\left(\frac{23}{29}\right) = \left(\frac{29}{23}\right) = \left(\frac{6}{23}\right) = \left(\frac{2}{23}\right) \cdot \left(\frac{3}{23}\right).$$

$23 \equiv 7 \mod 8$ so the first term is 1. And $\frac{3-1}{2} \cdot \frac{23-1}{2}$ is odd so

$$\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$$

since $3 \equiv 3 \mod 8$.

One problem with all this, of course, is the number of factors involved and, most importantly, the initial factorization step, required to use the Legendre symbols as we have done.

A second problem is that once you know a number is a p-quadratic residue, how do you find its root?

The answer to the first issue is found in the next section. One answer to the second question will be found in the section after that. There, the Tonelli-Shanks Algorithm gives a "successive approximation" method that converges in polynomial time.

21. **The Jacobi Symbol and its Reciprocity Law.**

The **Jacobi**[20] **Symbol** is defined in terms of Legendre Symbols, and its properties will allow us to calculate Legendre Symbols *much* more efficiently if the number involved is large with many factors.

If a is any positive integer coprime to $b = p_1 \cdot p_2 \cdots p_n$ where the p_i are odd primes we define the Jacobi Symbol $\left(\frac{a}{b}\right)$ by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_n}\right).$$

So if b happens to be prime then Legendre and Jacobi Symbols agree.

The following properties are obvious and require no proof beyond observation.

21.1. ***Lemma.*** *If a, b, c and d are positive integers and c and d are odd and ab is coprime to cd the following equalities hold for Jacobi Symbols (as we saw and used for Legendre Symbols earlier.)*

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right) \quad \textit{and} \quad \left(\frac{a}{cd}\right) = \left(\frac{a}{c}\right)\left(\frac{a}{d}\right).$$

and, whenever $a \equiv b \mod c$

$$\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right).$$

The following lemma is used to prove the main results in Theorem 21.3.

21.2. ***Lemma.*** *We suppose that $a_1, a_2, \ldots a_n$ are odd and exceed 2.*

$$\frac{a_1 \cdots a_n - 1}{2} \quad \textit{and} \quad \sum_{i=1}^{n} \frac{a_i - 1}{2} \quad \textit{are both even or both odd.}$$

$$\frac{(a_1 \cdots a_n)^2 - 1}{8} \quad \textit{and} \quad \sum_{i=1}^{n} \frac{a_i^2 - 1}{8} \quad \textit{are both even or both odd.}$$

Proof. Because both a_1 and a_2 are odd $\frac{(a_1-1)(a_2-1)}{2}$ is even and

$$\frac{(a_1-1)(a_2-1)}{2} = \frac{a_1 a_2 - 1}{2} - \left(\frac{a_1 - 1}{2} + \frac{a_2 - 1}{2}\right)$$

so the two terms on the right, which are both integers, are even or odd together.

[20]Carl Gustav Jacobi 1804-1851

Similarly, $\frac{(a_1^2-1)(a_2^2-1)}{8}$ is even and $\frac{a_1^2a_2^2-1}{8}$ is a whole number, a fact which can be shown by expanding $(2k+1)^2(2j+1)^2-1$ and observing it is always a multiple of 8. Also

$$\frac{(a_1^2-1)(a_2^2-1)}{8} = \frac{a_1^2a_2^2-1}{8} - \frac{(a_1^2-1)+(a_2^2-1)}{8}$$

so the second fraction on the right must be a whole number too and the two terms are even or odd whole numbers together.

We have proven both parts of the lemma for the case $n = 2$.

Suppose now we have proven the lemma for the case of $n = k \geq 2$ and $a_1, a_2, \ldots, a_{k+1}$ are odd. Let b be the odd number $a_1 \cdot a_2 \cdots a_k$. By inductive assumption

$$\frac{b \cdot a_{k+1}-1}{2} \quad \text{and} \quad \frac{b-1}{2} + \frac{a_{k+1}-1}{2} \quad \text{are both even or both odd and}$$

$$\frac{(b \cdot a_{k+1})^2-1}{8} \quad \text{and} \quad \frac{b^2-1}{8} + \frac{a_{k+1}^2-1}{8} \quad \text{are both even or both odd}$$

and the terms $\frac{b^2-1}{8}$ and $\frac{a_{k+1}^2-1}{8}$ are both whole numbers as are, more obviously, $\frac{b-1}{2}$ and $\frac{a_{k+1}-1}{2}$.

The results of the lemma now follow by replacing the integers $\frac{b-1}{2}$ and $\frac{b^2-1}{8}$ by the appropriate sums involving a_1, a_2, …, a_k, using the inductive assumption that the lemma is true for k factors as a guarantor that "evenness or oddness" of the term being replaced is retained. □

Using the lemma, it now follows that Legendre and Jacobi Symbols share other key properties besides those listed in Lemma 21.1, including a **Law of Quadratic Reciprocity** for Jacobi Symbols.

21.3. ***Theorem.*** *If a and c are distinct coprime odd positive integers then*

$$\textit{(i)} \qquad \left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}}$$

$$\textit{(ii)} \qquad \left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}}$$

$$\textit{(iii)} \qquad \left(\frac{a}{c}\right) \cdot \left(\frac{c}{a}\right) = (-1)^{\frac{c-1}{2}\cdot\frac{a-1}{2}}.$$

Proof. (i) Suppose $a = a_1 \cdots a_n$ and $c = c_1 \cdots c_k$ expresses the odd positive numbers a and c as the product of primes. Then

$$\left(\frac{-1}{c}\right) = \left(\frac{-1}{c_1}\right) \cdot \left(\frac{-1}{c_2}\right) \cdots \left(\frac{-1}{c_k}\right) = (-1)^{\frac{c_1-1}{2}}(-1)^{\frac{c_2-1}{2}} \cdots (-1)^{\frac{c_k-1}{2}}$$
$$= (-1)^{\sum_{i=1}^{k}\frac{c_i-1}{2}} = (-1)^{\frac{c_1\cdot c_2\cdots c_k-1}{2}} = (-1)^{\frac{c-1}{2}}$$

where the second to last equality in the last line follows from Lemma 21.2.

The proof of (ii) is identical.

(iii) is a little trickier. Suppose $c = c_1$ is prime. We have

$$\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) = \left(\frac{a_1}{c}\right)\left(\frac{a_2}{c}\right)\cdots\left(\frac{a_n}{c}\right)\cdot\left(\frac{c}{a_1}\right)\left(\frac{c}{a_2}\right)\cdots\left(\frac{c}{a_n}\right).$$

Pairing the terms involving specific a_i we have

$$\begin{aligned}\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) &= (-1)^{\frac{c-1}{2}\cdot\frac{a_1-1}{2}}\cdots(-1)^{\frac{c-1}{2}\cdot\frac{a_n-1}{2}}\\ &= (-1)^{\frac{c-1}{2}\cdot\left(\sum_{i=1}^{n}\frac{a_i-1}{2}\right)} = (-1)^{\frac{c-1}{2}\cdot\frac{a-1}{2}}\end{aligned}$$

with the last equality following, again, from Lemma 21.2. So we have the result for any odd a coprime to odd prime c.

But now for any $c = c_1\cdots c_k$ coprime to any odd a we have

$$\begin{aligned}\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) &= \left(\frac{a}{c_1}\right)\left(\frac{a}{c_2}\right)\cdots\left(\frac{a}{c_k}\right)\cdot\left(\frac{c_1}{a}\right)\left(\frac{c_2}{a}\right)\cdots\left(\frac{c_k}{a}\right)\\ &= (-1)^{\frac{c_1-1}{2}\cdot\frac{a-1}{2}}\cdot(-1)^{\frac{c_2-1}{2}\cdot\frac{a-1}{2}}\cdots(-1)^{\frac{c_k-1}{2}\cdot\frac{a-1}{2}}\\ &= (-1)^{\left(\sum_{i=1}^{k}\frac{c_i-1}{2}\right)\cdot\frac{a-1}{2}} = (-1)^{\frac{c-1}{2}\cdot\frac{a-1}{2}}.\end{aligned}$$

21.4. **Remark**. Recall the calculations in Remark 20.2. Let's use Jacobi Symbols to calculate whether -59850 is a 29-quadratic residue without factoring except to remove factors of 2.

$-59850 = (-1)\cdot 2\cdot 29925$ and by division $29925 = 1031\cdot 29 + 26$. So

$$\begin{aligned}\left(\frac{-59850}{29}\right) &= \left(\frac{-1}{29}\right)\left(\frac{2}{29}\right)\left(\frac{26}{29}\right) = \left(\frac{-1}{29}\right)\left(\frac{2}{29}\right)\left(\frac{2}{29}\right)\left(\frac{13}{29}\right)\\ &= \left(\frac{13}{29}\right) = \left(\frac{29}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1.\end{aligned}$$

One potential issue when doing the calculation above involves replacing $\left(\frac{a}{b}\right)$ by $\left(\frac{b}{a}\right)$ when a is coprime to b and b is larger than a. The next step is to write $b = ka + r$ and replace $\left(\frac{b}{a}\right)$ by $\left(\frac{r}{a}\right)$. We observe here the obvious fact that if a and r have a nontrivial common factor so too would the pair a and b.

So if a and b start out coprime none of the subsequent steps in the calculation will produce a pair of integers upon which the Jacobi Symbol is to be evaluated that *fail* to be coprime.

□

22. **The Tonelli-Shanks Algorithm for Producing Square Roots.**

If you somehow determine that a actually is a p-quadratic residue, the problem of how to *calculate* a square root of a mod p remains.

One approach would be to pick a member of Int_p and examine all its even powers till $a + kp$ appears for some k, an obvious non-starter if p is large.

Any odd prime p is of the form $1 + 4k$ or $3 + 4k$.

If $p = 3 + 4k$ then let $r = a^{\frac{p+1}{4}}$. That exponent is a whole number which allows us to evaluate it in principle. It can also be evaluated in practice in a reasonable amount of time. Any positive power of any number mod p can, a fact that is useful more generally.

Suppose n is a positive integer. Then writing n in base 2 we have

$n = 2^j + a_{j-1}2^{j-1} + \cdots + a_1 \cdot 2 + a_0$ for certain a_i all either 0 or 1.

$j + 1$ is the number of digits in a representation of n in base 2.

a^n can be calculated by squaring a and then squaring the result and repeating this j times until a^{2^j} is reached. Multiplying this by some of the previously calculated powers (those for which $a_i \neq 0$) produces a^n in at most $2j$ multiplications rather than n multiplications.

In practice, after each step one would reduce the product integer mod p to keep the size of the numbers no larger than p.

This is called, in the business, "polynomial time" and is regarded as manageable and the process we have just described is called **the exponentiation algorithm.**

In any event, by Euler's Criterion r is seen to be a square root of a:

$$r^2 = \left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \mod p.$$

The other square root is $p - r$.

The problem remains of how to proceed when $p \equiv 1 \mod 4$.

Suppose a is a p-quadratic residue for such a p. Then $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

Half the members of $RelPrime_p$ are p-quadratic *non-residues.*

Find one, call it h. Then $h^{\frac{p-1}{2}} \equiv -1 \mod p$.

Write $p - 1$ in the form $s \cdot 2^r$ for odd s and $r \geq 2$.

We will create a sequence of "approximate square roots to a" which must terminate in no more than r steps at a true square root of a.

This is the **Tonelli-Shanks algorithm**[21].

Let x_0 be the mod p residue of $a^{\frac{s+1}{2}}$ and k the mod p residue of h^s.

[21]The algorithm was described by Alberto Tonelli in 1891 and placed in modern form by Daniel Shanks in 1973.

So $k^{2^r} \equiv h^{p-1} \equiv 1 \mod p$ and also

$$\left(\frac{x_0^2}{a}\right)^{2^{r-1}} \equiv a^{s \cdot 2^{r-1}} \equiv a^{\frac{p-1}{2}} \equiv 1 \mod p$$

because a is known to be a p-quadratic residue.

So we know the order of the element $\frac{x_0^2}{a}$ is a power of 2, say 2^{t_0} where t_0 cannot exceed $r-1$.

Suppose now that we have created x_i for which $\frac{x_i^2}{a}$ has order 2^{t_i} where $t_i \geq 0$, as we have done for $i = 0$.

If $t_i = 0$ we are done, because in that case $x_i^2 = a$ and we have found our square root. Otherwise $t_i \geq 1$ and we proceed as follows.

Define x_{i+1} be the mod p residue of $x_i \cdot k^{2^{r-t_i-1}}$.

$$\left(\frac{x_{i+1}^2}{a}\right)^{2^{t_i-1}} \equiv \left(\frac{x_i^2 \left(k^{2^{r-t_i-1}}\right)^2}{a}\right)^{2^{t_i-1}} \equiv \left(\frac{x_i^2}{a}\right)^{2^{t_i-1}} \cdot \left(k^{2^{r-t_i}}\right)^{2^{t_i-1}}$$

$$\equiv \left(\frac{x_i^2}{a}\right)^{2^{t_i-1}} \cdot k^{2^{r-1}} \equiv (-1)(-1) \equiv 1 \mod p$$

where the (-1) equivalencies are due to the fact that $\frac{x_{i+1}^2}{a}$ has order exactly (not less than) 2^{t_i} and $k^{2^{r-1}} \equiv h^{\frac{p-1}{2}} \equiv -1 \mod p$.

It follows that $\frac{x_{i+1}}{a}$ has order dividing 2^{t_i-1}. Choose t_{i+1} so that $2^{t_{i+1}}$ is that order. So $t_{i+1} < t_i$.

We iterate for n steps until $t_n = 0$. The number n cannot exceed r. Then x_n and $p - x_n$ are the two mod p square roots of a.

r itself cannot exceed the number of digits in the binary representation of $p-1$. Using an efficient method to calculate powers (needed to determine $x_{i+1} \equiv x_i \cdot k^{2^{r-t_i-1}}$ and the exact order of x_{i+1}) each step takes polynomial time. So the Tonelli-Shanks algorithm itself takes polynomial time to implement.

There is a probabilistic component here: the selection of a p-quadratic non-residue h. Half the members of $RelPrime_p$ are non-residues, but there is no absolute guarantee that your first try, or any number of tries up to $\frac{p-1}{2}$, will succeed in finding one. The probability of success in n attempts to locate a non-residue exceeds $1 - \frac{1}{2^n}$ so this may not be a real worry in practice.

23. **Public Key Encryption.**

Our goal here is to understand some of the issues involved in modern encryption technology and, in particular, we describe a version of the **RSA cryptosystem** below.[22]

The purpose of encryption is to conceal the meaning of a message from those not authorized by the sender to have that message.

One ancient means of encryption is to simply disguise the letters of the message. For instance the table

$$\begin{array}{llllll} A\ 01 & B\ 02 & C\ 03 & D\ 04 & E\ 05 & F\ 06 \\ G\ 07 & H\ 08 & I\ 09 & J\ 10 & K\ 11 & L\ 12 \\ M\ 13 & N\ 14 & O\ 15 & P\ 16 & Q\ 17 & R\ 18 \\ S\ 19 & T\ 20 & U\ 21 & V\ 22 & W\ 23 & X\ 24 \\ Y\ 25 & Z\ 26 & & & & \end{array}$$

allows us to disguise "SECRETDECODERRING" as

"19050318052004050315040518180914 07".

This primitive method of disguising the meaning of the message could not fool anyone for long, so "encoded" messages of this kind as well as the original message would both be called "**plaintext**." It is our goal to discover a general method that could turn plaintext, which anyone can understand with more or less effort, into "**ciphertext**" which no one, not even the NSA, can turn back into plaintext by any known method without your permission. The process of creating ciphertext from plaintext is called **encryption**. The process of turning ciphertext into plaintext is called **decryption**.

Here are the "nuts and bolts" of such a process. You can estimate by what we know and the comments below that the tasks you are required to perform at each step can be done, and that factoring the integers involved cannot be done, by any known method in a practical amount of time (i.e. *polynomial* time) for numbers in the range of thousands of digits.

First we create the public/private key-pair to set up the encryption system. This is done once and used for any number of encrypted messages. Second, the sender encrypts and the receiver decrypts a message.

(1a) Produce distinct large primes p and q. Let $n = pq$ and calculate $\phi(n) = (p-1)(q-1)$. We will also need a number w which must be relatively prime to $\phi(n)$. For instance w could be a third prime and we make this choice. To avoid values which are too small or unnecessarily large we will choose w so that $\sqrt{\phi(n)} < w < \phi(n)$.

[22]RSA refers to the names of mathematicians Ron Rivest, Adi Shamir, and Leonard Adleman who publicized the algorithm in 1978. Apparently the method was invented (published in documents classified by the British government) in 1973 by the English mathematician Clifford Cocks.

(1b) Calculate d and k with $0 < d < \phi(n)$ and $wd + k\phi(n) = 1$.

(1c) Destroy all record of p, q, k and $\phi(n)$. Give the intended recipient of the encrypted messages the **private key** d using a very private and secure method. Destroy all other record of d. Make generally available the **public key** consisting of the two numbers w and n.

(2a) Encryption: Turn your message into a plaintext number and break it into pieces smaller than n. Let message m be one of these pieces of plaintext, which we assume to be neither 1 nor any multiple of p or q[23]. . Note $m^{\phi(n)} \equiv 1 \mod n$. Calculate the unique number $c \equiv m^w \mod n$ with $0 < c < n$. c is the ciphertext. Send c to the private key holder by any means you like.

(2b) Decryption: The private keyholder calculates the unique number $\overline{m} \equiv c^d \mod n$ with $0 < \overline{m} < n$. The number $\overline{m}$ is m and the message is decrypted.

That is all there is to it in practice, though some comments on the steps listed above are in order.

(1a) To get started, we must produce large primes p, q and w. The level of security in the encryption scheme is dependent on their size, so we require them to have binary representation longer than some predetermined number (typically thousands) of binary digits.

Large primes are common. If $\boldsymbol{\pi(n)}$ is the number of primes not exceeding n then

$$\lim_{n\to\infty} \frac{\pi(n)\ \ln(n)}{n} = 1 \qquad (\ln(n) \text{ is the natural log of } n.)$$

This is the **Prime Number Theorem** and was proved by both Hadamard and de la Vallée Poussin in 1896 using techniques invented by Riemann and his Riemann zeta function.[24]

So the probability that a randomly selected integer of size no larger than n is prime is roughly $1/\ln(n)$ for large n. This tells us how many numbers of a specified size we should expect to examine before finding a prime, and this number is manageable, even for huge n. But this result only talks about *limits* and we need specificity.

A far more informative result (from a practical standpoint) was proved by Pierre Dusart in 2010 who showed that

$$\frac{n}{\ln(n) - 1} < \pi(n) < \frac{n}{\ln(n) - 1.1}$$

[23]If p and q are in the neighborhood of a thousand digits, what is the probability that some random message violates this constraint? How could you know, before sending the message, if it was a "problem" m value? How would you "fix it" if by some extreme fluke your message happens to be a number that *does*?

[24]The mathematicians mentioned here are Jacques Hadamard 1865-1963 and Charles Jean de la Vallée Poussin 1866-1962 and the great Bernhard Riemann 1826-1866.

where the first inequality holds for $n \geq 5393$ and the second for $n \geq 60184$.

A candidate prime j of proper size is **randomly** selected. If j is prime then $m^j \equiv m \mod j$ for all m with $1 \leq m < j$. Even if j is not prime, it still could happen that $m^j \equiv m \mod j$ for a positive value (or even all positive values[25]) of m coprime to j. Candidate primes j are tested one after another until one is found that "passes this test," called the **Fermat Test**, for a **sufficient number** of **randomly chosen** different coprime numbers m. When that happens j is simply assumed to be prime: an "Industrial Grade Prime" or **Fermat pseudoprime**, if not an actual prime.[26] It is nowadays not hard to produce numbers with binary representation having length beyond a thousand digits and which have an **extremely high probability** of being prime. Encryption keys are formed using these.

(1b) Calculate d and k with $wd + k\phi(n) = 1$ using Euclid's algorithm. Select d so that $0 < d < \phi(n)$.

(1c) If the public could factorize n it would know $\phi(n)$ and therefore the private key d. The key to the security of this system is **only the apparently intractable problem of factoring large integers**. It seems that no one knows how to factorize n without exhaustively examining the potential **keyspace** to determine factors: all numbers, essentially, up to $\sqrt{n}$. To factorize an integer without small factors whose binary representation contains 128 digits would seem to require around six months if potential factors were checked at a rate of 10^{12} per second. Using 2048 digits creates a keyspace more than 10^{250} times larger. The "exhaustion" method of factorization, I think it is safe to say, cannot crack such an integer during the lifetime of our species. However no one has proven that factorization cannot be accomplished by some alternative, faster, method. This would break the RSA cryptosystem. If you discover such a method you are well advised to consider carefully who to tell, and how to tell them.

(2a) To encrypt, we will indicate how to efficiently calculate $c \equiv m^w \mod n$ with an example.

---

[25]Such numbers are called Carmichael numbers. The smallest is $561 = 3 \cdot 11 \cdot 17$, found by Robert Carmichael in 1910. There are an infinite number of these, but they become very scarce as their size increases. Exactly *how scarce* is an important and open question. For instance, numerical studies find that the probability that a randomly chosen number less than $n = 10^{21}$ is Carmichael is about 1 in $5 \cdot 10^{13}$. In 1956 Paul Erdös 1913-1996 proved that there is a positive constant k so that this probability cannot exceed $\exp\left(\frac{-k \cdot \ln(n) \cdot \ln\ln\ln(n)}{\ln\ln(n)}\right)$ for *any* n. There is good reason to suspect that k is at least 1. For a number n with 300 decimal digits and if $k = 1$ this probability is about $1.9 \cdot 10^{-29}$.

[26]The quality of the pseudoprime (that is, the probability that it is an actual prime) depends on the number of times it was tested and found to be "prime-like." If a number is *not* a Carmichael number and *not* a prime then it will fail the Fermat primality test for at least half of the smaller coprime m values, a fact that follows from Corollary 10.8. So if it is *not* a Carmichael number, after passing t "Fermat tests" the probability that it is prime is *at least* $1 - 1/2^t$.

(2b) To decrypt we need to calculate $m \equiv c^d \mod n$ by the same method.

To see that $\overline{m} = m$ we note that $0 < \overline{m} < n$ and

$$\overline{m} \equiv c^d \equiv (m^w)^d \equiv m^{1-k\phi(n)} \equiv m\left(m^{\phi(n)}\right)^{-k} \equiv m(1)^{-k} \equiv m \mod n.$$

Given the size restrictions on m and $\overline{m}$ this means they are equal.

23.1. **Remark**. There is complete symmetry between private and public key. In the example above we used a public key to encrypt information only one private key can decrypt. But a private key could be used to encrypt information that only the paired public key could decrypt. You as a ciphertext recipient want to be sure the message you decrypt actually came from the right person, and is not a fake message. After all, anyone can use your public key to create a message only you can decrypt. How would you modify the encryption system so you can be sure only the expected person could have sent it? This is the process of creating a **digital signature** to verify the authenticity of documents, and is a vital part of any cryptosystem. (hint: Each person in an exchange can create their own key-pair.)

24. An Example of Encryption.

First we create a public-private key-pair.

The key-pair maker[27] chooses primes $p = 101$ and $q = 107$. So $n = p \cdot q = 10807$. This number should be large enough to defy any known means of factorization, but of course here it can easily be factored.

Then $\phi(n) = 10600$ and w, a number relatively prime to $\phi(n)$, is selected. Let's pick $w = 113$.

Calculate d and k for which

$$113 \cdot d + k \cdot 10600 = 1 \quad \text{and} \quad 0 < d < 10600.$$

We saw in Remark 4.18 that $d = 3377$ and $k = -36$, though all we need here is d.

The private keyholder is given and retains (securely) the private key $d = 3377$. The numbers $w = 113$ and $n = 10807$ are distributed to any potential message senders. These last two numbers constitute the public key. $\phi(n) = 10600$ has served its purpose. The key-pair maker discards $\phi(n)$ and the private key d as well.

The only record of the private key must be in one or more secure locations, accessible to the private keyholder but not to the public.

[27]Often the key-pair maker is an application on the private keyholder's computer, and once the key pair is constructed the public key is uploaded to a library of public keys accessible to anyone and searchable by name or email address of the private keyholder.

Let's say our private keyholder has done all this, and we want to secretly send the message 100 to him or her.

We calculate $100^{113} \mod 10807$ to create ciphertext $c = 8382$. We send this ciphertext over a possibly insecure channel.

Our friend, who alone possesses the key d, calculates $8382^{3377} \mod 10807$. It is 100 and the plaintext is recovered.

There is only one small wrinkle here: how does one calculate these huge powers mod 10807? The **exponentiation algorithm** accomplishes this, as illustrated below.

The two residues we must calculate to follow the instructions from above are the residues of the numbers

$$100^{113} = 100^{64} \cdot 100^{32} \cdot 100^{16} \cdot 100 \qquad \text{and}$$

$$8382^{3377} = 8382^{2048} \cdot 8382^{1024} \cdot 8382^{256} \cdot 8382^{32} \cdot 8382^{16} \cdot 8382.$$

With numbers of this size you can actually use a calculator to keep track and do the calculations in a few minutes, though it would be a modest job to program the work on a computer.

To find the residue of a with modulus n for large a simply calculate the integer part, k, of a/n. So $a - k \cdot n$ (which is less than n) is the number you want.

We use a table to keep track of residues with modulus 10807:

$$100^4 \equiv 2829 \quad 100^8 \equiv 6061 \quad 100^{16} \equiv 2728 \quad 100^{32} \equiv 6768 \quad 100^{64} \equiv 5758.$$

$$\begin{array}{llll} 8382^2 \equiv 1617 & 8382^4 \equiv 10202 & 8382^8 \equiv 9394 & 8382^{16} \equiv 8081 \\ 8382^{32} \equiv 6667 & 8382^{64} \equiv 10505 & 8382^{128} \equiv 4748 & 8382^{256} \equiv 102 \\ 8382^{512} \equiv 10404 & 8382^{1024} \equiv 304 & 8382^{2048} \equiv 5960 & \end{array}$$

It still takes a while, but all the work shown above can be done in ten minutes with a calculator if you are efficient.

Now we have

$$\begin{aligned} 100^{113} &= 100^{64} \cdot 100^{32} \cdot 100^{16} \cdot 100 \\ &\equiv 5758 \cdot 6768 \cdot 2728 \cdot 100 \equiv 102 \cdot 2728 \cdot 100 \equiv 8081 \cdot 100 \equiv 8382 \end{aligned}$$

and

$$\begin{aligned} 8382^{3377} &= 8382^{2048} \cdot 8382^{1024} \cdot 8382^{256} \cdot 8382^{32} \cdot 8382^{16} \cdot 8382 \\ &\equiv 5960 \cdot 304 \cdot 102 \cdot 6667 \cdot 8081 \cdot 8382 \\ &\equiv 7980 \cdot 6667 \cdot 8081 \cdot 8382 \equiv 10606 \cdot 8081 \cdot 8382 \\ &\equiv 7576 \cdot 8382 \equiv 100. \end{aligned}$$

For practice, decrypt the ciphertext 4243 and turn it into legible English.[28]

[28]It is interesting that for all even powers of 4243 the second two digits of the four-digit residuals form a number that is 1 larger than the first two. And even powers of a number like 8383 have residuals with repeating pairs of digits. Do you know why?

References

[Bur07] David M. Burton. *Elementary Number Theory*. McGraw-Hill, 6th edition, 2007.
[Her75] I. N. Herstein. *Topics in Algebra*. Xerox College Publishing, 2nd edition, 1975.
[HW79] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 5th edition, 1979.
[NZ62] Ivan Niven and Herbert Zuckerman. *An Introduction to the Theory of Numbers*. John Wiley and Sons, 1962.

Index