# A FEW FACTS REGARDING NUMBER THEORY

LARRY SUSANKA

Contents



*Date*: May 13, 2018.

## 1. **Notation.**

We assume given and understood the set of integers $\mathbb{Z}$, sometimes denoted

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

We assume to be known the operations of addition and multiplication on integers and their basic properties, and 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." |

## 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 results in this section if you wish. Up to Section 9 (where you do calculations but must accept some statements on faith) declarative statements in the text and theorems, lemmas, propositions and corollaries in the later sections are all to be proven or justified by the interested student. These notes, from Remark 3.2 onward, are to be regarded as one long exercise.

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

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

2.7. ***Theorem.*** *Suppose* $a, b$ *and* $m$ *are positive integers.*
*(i)* $a \leq b \Leftrightarrow a + m \leq b + m$.
*(ii)* $ab \geq am \Leftrightarrow b \geq m$.
*(iii) If* $m = ab$ *then both* $a \leq m$ *and* $b \leq m$. *And if* $a > 1$ *then* $b < m$.

## 3. **Greatest Common Divisor and Least Common Multiple.**

3.1. **Definition**. We write $a|b$ (read as " $a$ divides $b$") when $a \neq 0$ and $b = ka$ for some $k$. We write $a \not| b$ when $a \neq 0$ and $b = ka + r$ for some $k$ and $r$ with $0 < r < |a|$.

3.2. **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 $a \not| b$.
(iii) If $a|b$ and $b|a$ then $a = \pm b$.

3.3. **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 $n$.

3.4. ***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) $j\mathbb{Z} + k\mathbb{Z} = k\mathbb{Z} \Leftrightarrow j\mathbb{Z} \subset k\mathbb{Z}$.*

3.5. ***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 $S \subset n\mathbb{Z}$. □

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

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

3.8. **Definition**. Suppose $a, b$ are not both 0. We write $d = gcd(a, b)$ 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 of $a$ and $b$.

3.9. ***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 $n = \pm d$.*

3.10. **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.

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

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

3.13. **Definition**. Suppose $a_1, \ldots, a_k$ are all nonzero for some $k > 2$. We write $d = gcd(a_1, \ldots, a_k)$ when $d|a_i \forall i$ and whenever $c|a_i \forall i$ then $c|d$. The number $d$ is called the greatest common divisor of these $a_i$.

3.14. ***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 $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} = d\mathbb{Z}$.*

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

3.16. ***Lemma.*** *(i) If $gcd(a, b) = d$ then $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

*(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*

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

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

3.18. **Remark**. Iterating the calculation identified in Theorem 3.17 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. Lamé showed that the implied procedure will terminate at the greatest common divisor after no more than five times the number of digits (base 10) of the smaller integer.

As an example we produce $gcd(11, 10600)$.

Using long division we find, successively:

$$10600 = 963 \cdot 11 + 7, \quad 11 = 1 \cdot 7 + 4, \quad 7 = 1 \cdot 4 + 3, \quad 4 = 1 \cdot 3 + 1.$$

This means

$$gcd(11, 10600) = gcd(11, 7) = gcd(7, 4) = gcd(4, 3) = gcd(3, 1)$$

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

But working backwards we also have

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2(11 - 7) - 7 \\ &= 2 \cdot 11 - 3 \cdot 7 = 2 \cdot 11 - 3 \cdot (10600 - 963 \cdot 11) \\ &= 2891 \cdot 11 - 3 \cdot 10600 \end{aligned}$$

which produces 1 as the required combination of 11 and 10600.

3.19. **Definition**. If $a$ and $b$ are nonzero we write $lcm(a, b) = m$ 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 of $a$ and $b$.

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

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

## 4. Linear Diophantine Equations.

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

4.2. ***Proposition.*** *The Diophantine 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 themselves solutions for every $t$.*

4.3. **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 4.2.

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.

## 5. **Prime Factorization.**

5.1. **Definition**. A number $p > 1$ is called prime if $a|p \Rightarrow a = \pm 1$ or $a = \pm p$. A positive number that is not prime is called composite.

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

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

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

5.4. ***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 $i$.*

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

5.6. **Remark**. Theorem 5.5 is proved by induction.

5.7. **Remark**. There are an infinitude of distinct primes.

## 6. **mod n Arithmetic.**

6.1. **Definition**. When $n > 1$ we write $a \equiv b \ mod \ n$ 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

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

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

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. We say a solution is unique *mod* $n$ if all solutions have the same residue.

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

6.3. ***Theorem.*** *If* $d = gcd(c, n)$ *then* $ca \equiv cb \ mod \ n$
*exactly when* $a \equiv b \ mod \ \frac{n}{d}$

6.4. **Remark**. Theorem 6.3 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 $d = 1$, you can do it.

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

6.5. **Definition**. We define, for integers $m$ and $k$ the set

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

Each integer is in one and only one of the sets

$$k\mathbb{Z}, \quad 1 + k\mathbb{Z}, \quad 2 + k\mathbb{Z}, \quad \ldots \quad (k-1) + k\mathbb{Z}$$

each of which consists of numbers with shared residue *mod* $k$ and which are called the congruency or residue (synonymous) classes *mod* $k$.

6.6. **Remark**. Note that if $\overline{m} = m + sk$ and $\overline{n} = n + uk$ then

$$\overline{m} + \overline{n} = (m + sk) + (n + uk) = (m + n) + (s + u)k$$

and also

$$\overline{mn} = (m + sk)(n + uk) = (mn) + (sn + um + suk)k.$$

We conclude that $\overline{m} + \overline{n} \equiv m + n \ mod \ k$ and $\overline{mn} \equiv mn \ mod \ k$.

6.7. **Definition**. Given residue classes $m + k\mathbb{Z}$ and $n + k\mathbb{Z}$ define

$$(m + k\mathbb{Z}) + (n + k\mathbb{Z}) = (m + n) + k\mathbb{Z}$$

and also

$$(m + k\mathbb{Z})(n + k\mathbb{Z}) = (mn) + k\mathbb{Z}.$$

In view of Remark 6.6, 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.

## 7. **The Chinese Remainder Theorem.**

7.1. ***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 one of the solutions*

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

*where $x_0$, $y_0$ is any particular solution to*

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

*and which can be found as suggested in Remark 4.3.*

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

7.3. **Remark**. Corollary 7.2 tells us that every number relatively prime to $n$ has one *mod* $n$ multiplicative inverse. But if $gcd(a, n) \not\equiv 1 \ mod \ n$ then $a$ does *not* have a *mod* $n$ multiplicative inverse.

7.4. ***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*

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

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

7.5. **Remark**. The proof of this result is instructive and proceeds as follows.

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 $mod \ n$.

7.6. **Remark**. In the Chinese Remainder Theorem it is necessary that the $n_i$ be pairwise relatively prime. There are systems with no solution otherwise.

## 8. **Fermat's Little Theorem.**

8.1. ***Theorem.*** *Fermat's Little Theorem:*
*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 by induction on $a$. □

8.2. ***Corollary.*** *If $p$ is prime and $a \not\equiv 0 \ mod \ p$ then $a^{p-1} \equiv 1 \ mod \ p$.*

8.3. **Definition**. For a given positive number $n$, $\phi(n)$ is the number of positive numbers less than $n$ and relatively prime to $n$. Obviously, if $p$ is prime $\phi(p) = p-1$. It is not hard to show that $\phi(p^k) = (p-1)p^{k-1}$ for prime $p$ and $k > 0$. Also, if $p$ and $q$ are distinct primes that $\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$.

In fact, more is true: $\phi(mn) = \phi(m)\phi(n)$ whenever $m$ and $n$ are greater than 1 and relatively prime.

The theorem stated and proved below only in the case of $n = pq$ is actually true for any $n \geq 2$.

8.4. ***Corollary.*** *If $p$ and $q$ are distinct primes and $n = pq$ then*

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

*Proof.* If $a$ is 1 or any multiple of $pq$ the result is obvious.

If $a$ is not 0 then

$$\left(a^{p-1}\right)^{q-1} \equiv 1 \ mod \ q \quad \text{and} \quad \left(a^{q-1}\right)^{p-1} \equiv 1 \ mod \ p.$$

That means $\left(a^{p-1}\right)^{q-1} - 1$ is divisible by both $p$ and $q$ and therefore divisible by the product $pq$. □

## 9. **Public Key Encryption.**

Our goal here is to understand some of the issues involved in modern encryption technology.

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

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

| | | | | | |
|---|---|---|---|---|---|
| $A$ 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 | | | | |

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 will simply have to take my word for it 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, for numbers in the range of thousands of digits.

(1) Produce two large primes $p$ and $q$. Let $n = pq$ and $\phi(n) = (p-1)(q-1)$.

(2) Pick $w$ relatively prime to $\phi(n)$. For instance $w$ could be any prime larger than $\sqrt{\phi(n)}$ but less than $\phi(n)$ itself so the numbers don't get too large.

(3) Calculate $d$ and $k$ with $0 < d < \phi(n)$ and $wd + k\phi(n) = 1$. (Note that $k$ must be negative under these conditions. We will not use $k$ in subsequent work.)

(4) Destroy all record of $p, q, k$ and $\phi(n)$. Give the intended recipient of the message 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 $n$.

(5) 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 nonzero. 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.

(6) 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.

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

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 $2 \leq m < j$. Even if $j$ is not prime, it still could happen that $m^j \equiv m \ mod \ j$ for any, or even all of, these values of $m$. But this is **very unlikely** if $j$ is large and this probability can be estimated. 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 different prime numbers $m$. When that happens $j$ is simply assumed to be prime: an "Industrial Grade Prime" if not an actual prime. 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.

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

(4) 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.

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

(6) 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

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

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

9.1. **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: You may create another key pair for your confederate.)

10. **An Example of Encryption.**

We choose primes $p = 101$ and $q = 107$. Let $n = pq = 10807$. We will normally need this number to be large enough to defy any known means of factorization, but of course here it can easily be factored.

We then calculate $\phi(n) = 10600$ and select relatively prime $w$. Let's pick $w = 11$.

Calculate $d$ and $k$ for which

$$11d + k\phi(n) = 1 \quad \text{and} \quad 0 < d < \phi(n).$$

We saw in Remark 3.18 that $d = 2891$ and $k = -3$, though all we need here is $d$.

Give the private key $d = 2891$ to the intended recipient only and broadcast $w = 11$ and $n = 10807$ however you like: these two numbers form the public key.

Let's say we want to secretly send the message 100 to our friend.

We calculate $100^{11}$ *mod* 10807 to create ciphertext $c = 2120$. We send this message over a possibly insecure channel.

Our friend who possesses the key $d$ calculates $2120^{2891}$ *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 two residues we must calculate to follow the instructions from above are

$$100^{11} = 100^8 \cdot 100^2 \cdot 100 \qquad \text{and}$$
$$2120^{2891} = 2120^{2048} \cdot 2120^{512} \cdot 2120^{256} \cdot 2120^{64} \cdot 2120^8 \cdot 2120^2 \cdot 2120.$$

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 $a - kn$ (which is less than $n$) is the number you want.

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

| | | | |
|---|---|---|---|
| $2120^2 \equiv 9495$ | $2120^4 \equiv 3031$ | $2120^8 \equiv 1011$ | $2120^{16} \equiv 6263$ |
| $2120^{32} \equiv 6566$ | $2120^{64} \equiv 3233$ | $2120^{128} \equiv 1920$ | $2120^{256} \equiv 1213$ |
| $2120^{512} \equiv 1617$ | $2120^{1024} \equiv 10202$ | $2120^{2048} \equiv 9394$ | |

$$100^4 \equiv 2829 \qquad 100^8 \equiv 6061$$

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

For practice, decrypt the ciphertext 2728 and turn it into legible English.