Elementary Number Theory: A Brief Introduction From Math 592 - Cryptography @ Eastern Michigan University

David Moll
dmoll@emich.edu

April 15, 2017

1 Introduction

The driving reason for putting together this set of notes is to provide a reference for myself that covers the basic facts and theorems of Number Theory, especially as they relate to the study of cryptography. With that in mind, I am only going to give a cursory treatment to some of the more basic theorems that form the underlying basis for the field, and focus primarily on those sections which have been less obvious to me personally - both now and in the past.

2 Divisibility

2.1 Definition

Let $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ be the *integers*. Suppose we have integers a and b, with $b \neq 0$. Then, we say that the integer a *divides* the integer b, written as $a|b$ if there exists an integer k such that $b = ak$.

2.2 Some rules about divisibility

1. $a|b$ and $b|c \rightarrow a|c$
2. $a|b$ and $b|a \rightarrow a = \pm b$
3. $a|b$ and $a|c \rightarrow a|(b + c)$ and $a|(b - c)$

2.2.1 Proof of Transitivity of Divisibility

Proof.

$a|b$ implies that $\exists k \in \mathbb{Z}$ such that $b = a \cdot k (a, b \neq 0)$ (by definition)
$b|c$ implies $\exists l \in \mathbb{Z}$ such that $c = b \cdot l$
$c = b \cdot l$
$c = a \cdot (k \cdot l)$ (because $b = a \cdot k$)
$a|c$ (by the definition of divisibility, because $k \cdot l \in \mathbb{Z}$)

□

3 Common Divisors

A common divisor of two integers a and b is a positive integer that divides them both. Formally, we would say that n is a common divisor of a and b if $\exists n \in \mathbb{Z}, n > 0$ where $n|a$ and $n|b$.

3.1 Greatest Common Divisor

The Greatest Common Divisor, or gcd of a and b is the largest integer that divides both a and b.

definition 1. Suppose a,b are both not 0.
$d = \gcd(a, b)$ is the greatest d contained in the set of divisors $\{d : d|a, d|b \text{ and } d > 0\}$

Proof. We want to show that this set of divisors has a maximum value - which is the gcd.

$a = d \cdot k$ and $b = d \cdot l$ for some $k, l \in \mathbb{Z}$
$|a| = |d| \cdot |k|$ and $|b| = |d| \cdot |l|$
Suppose $a \neq 0$, then $|d| \leq |k| \cdot |d| = |a|$
Thus, the set is bounded above (by a) and has a max value.

□

Note We can see that if $a, b \neq 0$, $\gcd(a, b) \leq \min(|a|, |b|)$

3.2 GCD Examples

3.2.1 Zero Case

1. $\gcd(0, 3) = 3$
2. $\gcd(0, 0) = 0$ (we define this for convenience)

3.2.2 Useful Examples

1. $\gcd(9, 3) = 3$
2. $\gcd(13, 7) = 1$
3. $\gcd(100, 25) = 5$
4. $\gcd(1432, 12488) = 8$
5. $\gcd(1432, 12489) = 1$

4 The Division Algorithm

4.1 This is simply a formal statement of the method for long division that we learned "long" ago.

The division algorithm is important, because it is the building block for methods and algorithms in later sections. Repeated application of the division algorithm is at the heart of the Euclidean Algorithm, which will give us a method for finding the GCD of two integers.

definition 2. Let a and b be positive integers. Then there are unique non-negative integers q and r such that:

$$a = q \cdot b + r \text{ and } 0 \leq r < b$$

4.2 Proof of the Division Algorithm

Our goal here is to show that q and r are unique for the above equation and that r satisfies the inequality.

Proof. Define $\mathbf{X} = \{a - bq : q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$
We can see that $\mathbf{X}$ is non-empty, since $\exists q \in \mathbb{Z}$ such that $a \geq bq$
And $\mathbf{X} \subseteq \mathbb{N}_0$. In particular, it is bounded below, and contains a least element, r.
$\therefore r = a - bq$ for some $q \in \mathbb{Z}$
Note: We know that $r \geq 0$, because $r \in \mathbf{X} \subseteq \mathbb{N}_0$

Now we want to examine the possibility that $r \geq b$

$$\begin{aligned} 0 &\leq r - b && \text{(Move both terms to one side)} \\ 0 &\leq (a - bq) - b && \text{(From above, } r = a - bq) \\ 0 &\leq a - b(q + 1) && \text{(Which is a member of } \mathbf{X} \text{ as it is of the form } a - bq) \end{aligned}$$

We can see that $a - b(q + 1) < r$, which contradicts the minimality of r.
$\therefore r < b$
To show that r and q are unique, suppose the following:
$a = bq' + r'$ and $0 \leq r' < b$

$$\begin{aligned} bq + r &= bq' + r' && \text{(We assume that these equations are equal)} \\ b(q - q') &= r' - r \\ b \cdot |q' - q| &= |r' - r| && \text{(We can take the absolute value to simplify our lives here} \\ b > |r' - r| &= b \cdot |q' - q| && \text{(Since } b > r) \\ 1 > |q' - q| &\geq 0 \end{aligned}$$

$\therefore q' - q = 0$ and $r' - r = 0$, so q and r are unique. □

5 Integer Linear Combinations

definition 3. An integer m is an **integer linear combination** of two integers a and b if:

$$m = ax + by$$

for some pair of integers x and y.

Essentially, this is a one dimensional vector. We'll define $\mathbf{V} = \{ax + by : x, y \in \mathbb{Z}\}$ as the set of all integer linear combinations. We will note the two closure properties:

5.1 $m, m' \in \mathbf{V} \Rightarrow m + m' \in \mathbf{v}$

5.2 $m \in \mathbf{V}$ **and** $r \in \mathbb{Z} \Rightarrow r \cdot m \in \mathbf{V}$

And move on, as there isn't much more to say about these, except that we will use them in Bezout's Theorem.

6 Bezout's Theorem

Bezout's Theorem basically states than the GCD of two integers a and b can be represented as a linear combination of integers. This is a useful fact that allows us to derive rules about how gcds behave algebraically, and is crucial in proving some later theorems.

Theorem 4. *Let a,$b \in \mathbb{Z}$ with at least one of a and $b \neq 0$. We will define $\mathbf{V}^+ = \mathbf{V} \cap \mathbb{N}$, that is to say that $\mathbf{V}^+$ is the set of all positive linear integer combinations, so that $\mathbf{V}^+ \neq 0$, and it contains a minimal element γ.*
We define $\gamma = \gcd(a, b)$

Proof. Suppose $a \neq 0$ Then $|a| = \pm a \in \mathbf{V}^+$
Likewise, if $b \neq 0$ Then $|b| = \pm b \in \mathbf{V}^+$
So we know that $\mathbf{V}^+ \neq 0$. By the Least Integer Principle, $\mathbf{V}^+$ contains a minimal element γ. Since $\gamma \in \mathbf{V}^+$, we know that $\gamma = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$. If d is a common divisor of a and b, then $d|\gamma$. Given the case where $d = \gcd(a, b)$, we have that $\gcd(a, b)|\gamma$, which tells us that $\gcd(a, b) \leq \gamma$.
Now we want to show that γ is a common divisor of a and b, which will allow us to say that γ is less than or equal to the $\gcd(a, b)$, which when combined with the result we just derived will allow us to say definitively that $\gamma = \gcd(a, b)$.
We start with the division algorithm and write $a = q\gamma + r$ for $0 \leq r < \gamma$.
Solving for r gives us $r = a - q\gamma$
Since $a, \gamma \in \mathbf{V}^+$, we must have that $r \in \mathbf{V}^+$, but the result from **5.1** and **5.2**. As before, the possibility of $r > 0$ would contradict the minimality of γ. $\therefore r = 0$ or $\gamma|a$.
We can repeat the above with b instead of a to show that $\gamma|b$. Thus, γ is a common divisor and we can say that $\gcd(a, b) \geq \gamma$. $\therefore \gcd(a, b) = \gamma$ □

7 An Aside on GCDs and Divisibility

Now that we have some tools, we can define some identities and relations for how relatively prime integers interact with each other with respect to their divisibility.

Lemma 5. *Suppose a and b are relatively prime ($\gcd(a, b) = 1$), and that $a|bc$. Then $a|c$. (Given $a, b \in \mathbb{Z}, a, b \neq 0$).*

Proof.

$1 = ax + by$ for some $x, y \in \mathbb{Z}$	(By Bezout's theorem)
$c = acx + bcy$	(multiply both sides by c)
$c = acx + aky$	(Since $a\|bc \Rightarrow bc = ak$)

And we can see that $a|acx$ and $a|aky$, $\therefore a|c$ □

Lemma 6. *Suppose $a, b \in \mathbb{Z}$ and they are not both 0. If d is a common divisor of a and b, then $d|\gcd(a, b)$.*

Proof. By Bezout's theorem,

$$\gcd(a, b) = ax + by \text{ for some } x, y \in \mathbb{Z}$$

Since $d|a$ and $d|b$, we see that d divides the right side of the above equation, so it must also divide the left side of the above equation, which gives us our result that $d|\gcd(a, b)$. □

Lemma 7. *Suppose a and b are relatively prime. If $a|c$ and $b|c$ then $ab|c$.*

Proof.

$$
\begin{aligned}
1 &= ax + by \text{ for some } x, y \in \mathbb{Z} && \text{(By Bezout's theorem)} \\
c &= acx + bcy && \text{(multiply both sides by } c\text{)} \\
a|c &\Rightarrow ak = c \text{ for some } k \in \mathbb{Z} && \text{(Definition of divisibility} \\
b|c &\Rightarrow b\ell = c \text{ for some } \ell \in \mathbb{Z} \\
c &= ab\ell x + abky && \text{(Substituting in)} \\
c &= ab(lx + ky) && \text{(Note that } lx + ky \text{ is just an integer)} \\
\therefore ab|c
\end{aligned}
$$

□

Lemma 8. *Suppose c is a positive divisor of both a and b. Then $\gcd(a, b) = c \cdot \gcd(\frac{a}{c}, \frac{b}{c})$.*

This Lemma deserves a comment - it is basically saying that we can extract a factor from the two integers we are taking the GCD of. This will be a useful trick for later when we want to compute the GCD quickly.

Proof. We can define $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$. Now, we can divide everything by c, and we know that we still have integers. Our equation now looks like

$$
\begin{aligned}
\frac{1}{c}\gcd(a, b) &= \frac{a}{c}x + \frac{b}{c}y \\
\frac{a}{c}x + \frac{b}{c}y &\geq \gcd(\frac{a}{c}, \frac{b}{c}) && \text{(By Bezout's Theorem)} \\
\frac{1}{c}\gcd(a, b) &\geq \gcd(\frac{a}{c}, \frac{b}{c}) \\
\gcd(a, b) &\geq c \cdot \gcd(\frac{a}{c}, \frac{b}{c}) && \text{(Multiply both sides by } c\text{)}
\end{aligned}
$$

Here we're using one of our standard techniques for proving gcd identities - we work at it from both sides to show that the equations we want are both greater than AND less than each other, so they must be equal. Now we're going to work on showing the "less than" portion.

$$
\begin{aligned}
c \cdot \gcd(\frac{a}{c}, \frac{b}{c}) &= c \cdot (\frac{a}{c}x' + \frac{b}{c}y') && \text{(for some } x', y' \in \mathbb{Z}\text{)} \\
c \cdot \gcd(\frac{a}{c}, \frac{b}{c}) &= ax' + by' \\
ax' + by' &\geq \gcd(a, b) && \text{(By Bezout's Theorem)} \\
c \cdot \gcd(\frac{a}{c}, \frac{b}{c}) &\geq \gcd(a, b)
\end{aligned}
$$

So now we have shown $c \cdot \gcd(\frac{a}{c}, \frac{b}{c}) \geq \gcd(a, b)$ and $\gcd(a, b) \geq c \cdot \gcd(\frac{a}{c}, \frac{b}{c})$.

$\therefore \gcd(a, b) = c \cdot \gcd(\frac{a}{c}, \frac{b}{c})$.

□

8 Euclidean Algorithm

The Euclidean algorithm makes repeated use of the division algorithm, shifting q and r over at each step until $r = 0$, at which point q is the gcd of a and b. Let's write this out explicitly:

A method for calculating $\gcd(a, b)$

1. $r_0 = q_1 * r_1 + r_2$
2. $r_1 = q_2 * r_2 + r_3$
3. ...
4. $r_{n-2} = q_{n-1} * r_{n-1} + r_n$
5. $r_{n-1} = q_n * r_n + r_{n+1}$

At each state we are decreasing the value of r_i such that $0 \leq r_{i+1} < r_i$, so at some point $r_{n+1} = 0$. Which gives us our result that $r_n = \gcd(a, b)$ and we see that r_n can be expressed as a linear combination of a and b.

Why does this work? Look at the last step - $r_{n-1} = q_n * r_n + 0$, which implies that $r_n | r_{n-1}$. And then the previous step implies that $r_{n-1} | r_{n-2}$. This repeats all the way up to r_0, and by the transitive property of divisibility we see that r_n is a common divisor of r_1 and r_0, which correspond to a and b, $\therefore r_n \leq \gcd(a, b)$. Likewise, since $a = r_0$ and $b = r_1$, then $\gcd(a, b) | r_0$ and $\gcd(a, b) | r_1$, which gives us

1. $r_2 = r_0 - q_1 * r_1 \Rightarrow \gcd(a, b) | r_2$ because $\gcd(a, b)$ divides both terms on the right side of the equation
2. $r_3 = r_1 - q_2 * r_2 \Rightarrow \gcd(a, b) | r_3$
3. ...
4. $r_n = r_{n-2} - q_{n-1} * r_{n-1} \Rightarrow \gcd(a, b) | r_n$

Which tells us that $r_n \geq \gcd(a, b)$, where each row in the above sequence follows from the transitive property of divisibility. $\therefore r_n = \gcd(a, b)$

8.1 Examples of using the Euclidean Algorithm

$$a = 756, b = 45$$
$$756 = 16 \cdot 45 + 36$$
$$45 = 1 \cdot 36 + 9$$
$$36 = 4 \cdot 9 + 0$$

Thus when $r_{n+1} = 0$ we see than $r_n = 9$, so we know that $\gcd(756, 45) = 9$.

8.2 What's the Linear Integer Combination?

We can build back up from the last statement of the above example to get a linear integer combination for the gcd.

$$9 = 45 - 1 \cdot 36$$
$$9 = 45 - 1 \cdot (756 - 16 \cdot 45)$$
$$9 = 17 \cdot 45 - 1 \cdot 756$$

Breaking out our calculators, we see that this is $765 - 756 = 9$. So we have our linear integer combination of the form $\gcd(a, b) = ax + by$, where in this particular case $x = 17$ and $y = -1$.

9 Extended Euclidean Algorithm

If we have multiple steps in our process of finding the $\gcd$ through Euclid's Algorithm, it would be cumbersome to do the back substitution so that we could derive the integer linear combination of $ax + by = \gcd(a, b)$. Instead, we can use matrix multiplication to find the coefficients for Bezout's Theorem.

9.1 Using matrix multiplication to find coefficients for Bezout's Theorem

Define $Mq = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix}$ We know that we can use matrix multiplication to solve a series of linear equations, which is what we are doing when we are finding the coefficients for Bezout's Theorem. As such, starting with the knowledge that $gcd(a, b) = r_n$, we have: $\begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} = Mq_{n-1} \cdot Mq_{n-2} \cdot \ldots \cdot Mq_1 \begin{bmatrix} r_0 \\ r_1 \end{bmatrix}$

Performing all of the multiplication gives us the coeffients x and y as the bottom row of the resulting 2x2 matrix, since when all of the computations are finished, the bottom row works out to $r_n = x \cdot r_0 + y \cdot r_1$.

Let's do one example. Find the a linear integer combination for the $\gcd(123, 277)$

1. $277 = 2 \cdot 123 + 31$
2. $123 = 3 \cdot 31 + 30$
3. $31 = 1 \cdot 31 + 1$
4. $30 = 30 \cdot 1 + 0$

So we see that the $\gcd(123, 277) = 1$. Now let's find x and y such that $123x + 277y = 1$. We'll use matrix multiplication. We need to solve:

- $\begin{bmatrix} 30 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 277 \\ 123 \end{bmatrix}$
- Working out the multiplication gives us:
- $\begin{bmatrix} 30 \\ 1 \end{bmatrix} = \begin{bmatrix} -3 & 7 \\ 4 & -9 \end{bmatrix} \begin{bmatrix} 277 \\ 123 \end{bmatrix}$

Taking the bottom row we see that $1 = 4 \cdot 277 + (-9) \cdot 123$, which is our solution. See the appendix for python code that will perform this matrix multiplication. The nice thing about finding the gcd and coefficients this way is that because we're using matrix multiplication the algorithm uses constant memory.[1]

10 Congruences (a very useful form of myopia)

10.1 What are congruences?

We talk about congruences modulo n. These are actually Equivalence Classes mod n, but we won't dive into that right now. First, let's define a congruence.

definition 9. Given the set of integers $\mathbb{Z}$, choose a specific b in the set and divide it by n.
By the division algorithm, this gives us $b = qn + r$, where $r = 0, 1, 2, \ldots, n - 1$.
We can rewrite this as $b - r = qn$ Which is really saying that the difference between b and r is always an integer multiple of n. Hence we write:

$$b \equiv r mod n$$

And we say that b is equivalent to $rmodn$.

[1] Python code bezout.py taking from Dr. J Ramanatha's course website http://people.emich.edu/jramanath/docs/math409-592w17/bezout.py

11 Equivalence classes mod n

We know that a congruence mod n is an equivalence relation on $\mathbb{Z}$. For a particular $\mathbb{Z}$ modulo n, we write $\mathbb{Z}_n$, if we were to choose $n = 5$ we would write Z_5, and call it "$\mathbb{Z} \mod 5$". Z_5 is a set of equivalence classes, and we will denote these equivalence classes by underlining them. So we can say:

$$Z_5 = \{\underline{0}\,\underline{1}, \underline{2}, \underline{3}, \underline{4}\}$$

and in particular,

$$\begin{aligned}
\underline{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
\underline{1} &= \{\ldots, -9, -4, 0, 1, 6, \ldots\} \\
\underline{2} &= \{\ldots, -8, -3, 0, 2, 7, \ldots\} \\
\underline{3} &= \{\ldots, -7, -2, 0, 3, 8, \ldots\} \\
\underline{4} &= \{\ldots, -6, -1, 0, 4, 9, \ldots\}
\end{aligned}$$

We can see that each element of $\underline{1}$ when taken modulo 5 is equal to 1.

11.1 We can operate on congruence classes!

For multiplication:

$$\underline{2} \cdot \underline{4} = 8 \mod 5 = \underline{3}$$

For addition:

$$\underline{2} + \underline{4} = 6 \mod 5 = \underline{1}$$

Since congruences are closed under addition and multiplication (remember: we're in a ring), any addition or multiplication of these congruence classes (or elements from the congruence classes) will **by definition** keep us in the congruence modulo n that we started in.

12 Arithmetic in $\mathbb{Z}_n$

This is important, so we'll state it again - the definition of a congruence: Let n be a positive number and $a, b \in \mathbb{Z}$. Then we say that a is congruent to b modulo n if

$$n|(b-a)$$

which also means that $b - a = kn$ for some $k \in \mathbb{Z}$. And we write this as

$$a \equiv b \mod n$$

When we do arithmetic with congruences, we are doing arithmetic in $\mathbb{Z}_n$. So we'll do a quick proof that congruences are closed under addition and multiplication, even though we've been assuming it up to this point.

12.1 Proof of arithmetic rules in $\mathbb{Z}_n$

Proof. Show that if $a \equiv b \mod n$ and $c \equiv d \mod n$ then

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

$$\begin{aligned}
a \equiv b \mod n &\Rightarrow \exists k \in \mathbb{Z} \text{ such that } b - a = kn && \text{(by definition of a congruence)} \\
c \equiv d \mod n &\Rightarrow \exists l \in \mathbb{Z} \text{ such that } d - c = ln && \text{(by definition of a congruence)} \\
\therefore (b-a) + (c-d) &= (k+l) \cdot n \\
(b+d) - (a+c) &= (k+l) \cdot n && \text{(Rearrange terms in the order we want)}
\end{aligned}$$

This implies that $n|(b+d)-(a+c)$, which from the definition of a congruence gives us $a+c \equiv b+d \mod n$, which is what we were trying to prove. □

Proof. Show that if $a \equiv b \mod n$ and $c \equiv d \mod n$ then

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

The first two steps of this proof are identical to the above proof, so we'll omit them and start in on the meat of the argument.

$$\begin{aligned}(b \cdot d) - (a \cdot c) &= (bd - ad) + (ad - ac) && \text{(Here we add +ad and -ad to the two terms on the right side)}\\ &= (b-a)d + a(d-c) && \text{(Factor out like terms)}\\ &= (kd)n + (al)n && \text{(Substitute in from our definition and rearrange terms)}\\ (b \cdot d) - (a \cdot c) &= (kd + al)n && \text{(note that } kd + al \text{ is just an integer)}\end{aligned}$$

$\therefore n|(bd - ac)$ or $ac \equiv bd \mod n$ □

13 Units in $\mathbb{Z}_n$

definition 10. We say that a Congruence class $\underline{a}$ is **invertible** or is a **unit** if there is a congruence class $\underline{x}$ that satisfies the following equation:

$$\underline{ax} = \underline{1}$$

If $a \in \underline{a}$ and $x \in \underline{x}$ we can write instead

$$ax \equiv 1 \mod n$$

13.1 Examples

For $\mathbb{Z}_7$, the following three statements all mean the same thing!

- $\underline{3} \cdot \underline{4} = \underline{15} = \underline{1}$
- So $\underline{3}$ is invertible in $\mathbb{Z}_7$
- $3 \cdot 5 \equiv 15 \equiv 1 \mod 7$

Let's examine another example in $\mathbb{Z}_{12}$. Is 9 invertible in $\mathbb{Z}_{12}$?
Solve: $9x \equiv 1 \mod 12$
This would mean that $9x - 1 = 12k$ for some $k \in \mathbb{Z}$
The above statement implies that $3|1$, which isn't possible, so we have a contradiction.
$\therefore$ there are no solutions and 9 is not invertible in $\mathbb{Z}_{12}$

One last example where actually find an inverse!
Is 14 invertible in $\mathbb{Z}_{29}$? (note - observe that $\gcd(14, 29) = 1$)
So we know from Bezout's Theorem that there is an integer linear combination of 14 and 29 that yields 1. Thus, we can write

$$14x_0 + 29y_0 = 1$$

Now, we remember that *Congruences are a useful form of myopia*, and put our $\mathbb{Z}_{29}$ glasses on. This turns the equation into:

$$14x_0 \mod 29 + 29y_0 \mod 29 \equiv 1 \mod 29$$

Then we remember that $29 \cdot (blah) \mod 29 \equiv 0$ for any $blah$, and we can remove it from our equation to give us

$$14x_0 \equiv 1 \mod 29$$

And from Bezout's Theorem we know there's a solution, so a quick check shows us that $(-2)14 + (1)29 = 1$. Which tells us that

$$x_0 \equiv -2 \mod 29$$

$$x_0 \equiv 27 \mod 29 \quad \text{(We're shifting within our congruence class to the least positive member of the class)}$$

$\therefore 14 \cdot 27 \equiv 1 \mod 29$

13.2 Theorem on invertibility in $\mathbb{Z}_n$

Theorem 11. *$a \in \mathbb{Z}$ is invertible $\mod n$ if and only if $\gcd(a, n) = 1$*

Proof. Because this is an "if an only if" proof, we want to show $\Rightarrow$ and $\Leftarrow$. We'll show $\Rightarrow$ first.
Suppose a is invertible mod n.
Then $\exists x \in \mathbb{Z}$ such that $a \cdot x \equiv 1 \mod n$.
So from the definition of a congruence, we know that $n|(ax - 1)$
Which is equivalent to $ax - ny = 1$ for some $y \in \mathbb{Z}$ And we immediately see that 1 is the smallest positive linear combination of a and n, so $\gcd(a, n) = 1$ directly from Bezout's Theorem.
Now, focusing on $\Leftarrow$, supposed that $\gcd(a, n) - 1$. Thus, $ax + ny = 1$ for some $x, y \in \mathbb{Z}$ (again, from Bezout's Theorem - see how useful it is?)
When we put on our $\mod n$ glasses, $ax + ny = 1$ becomes $ax \equiv 1 \mod n$, because ny goes to 0 when viewed through the lens of $\mod n$.
$\therefore ax \equiv 1 mod n$ and we have shown if and only if. □

14 The Chinese Remainder Theorem

The Chinese Remainder Theorem provides us with a useful method for solving systems of congruences, given that certain conditions are met. This theorem has this name because it is a theorem about remainders, which was first discovered in the 3rd century AD by the Chinese mathematician Sunzi in Sunzi Suanjing.[2]

Theorem 12. *Suppose $n_1, N_2, \ldots, n_\ell$ are pairwise, relatively prime positive integers and $b_1, b_2, \ldots, b_\ell$ are arbitrary integers. Then, there is an $x \in \mathbb{Z}$ that is a solution to the system of equations:*

$$x \equiv b_i mod n_i for i = 1, \ldots, \ell$$

And the solution to this system is unique modulo $\mathbf{N} = n_1, n_2, \ldots, n_\ell$

14.1 Concrete example of what this means

Example 13. Suppose we have a system of congruences:

$$\begin{cases} x \equiv 5 \mod 11 \\ x \equiv 7 \mod 13 \end{cases}$$

The Chinese Remainder Theorem implies that a solution x_0 to this system exists, and that the full solution family (because the solution exists as a congruence class) has the form $x_0 + n \cdot 11 \cdot 13$, for some $n \in \mathbb{Z}$. Note that 11 and 13 are relatively prime to each other.

Now that we know what this would look like in practice, let's continue on and prove the theorem, which will also give us a method for finding a solution to the system of congruences.

Proof. The proof is by induction on ℓ, starting from $\ell = 2$.

Basis Step: Assume $\ell = 2$. Consider a system of the form:

$$\star = \begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \end{cases} \quad \text{where } gcd(n_1, n_2) = 1$$

Let $\alpha_1, \alpha_2 \in \mathbb{Z}$ such that $\alpha_1 n_1 + \alpha_2 n_2 = 1$ (from Bezout's Theorem)
Set $x = b_2 \alpha_1 n_1 + b_1 \alpha_2 n_2$

Note 14. We are sort of backing into this equation from the original system of congruences. Since with our $\mod n_1$ glasses on, the above equation becomes $x \equiv 0 + b_1 \cdot 1 = b_1 \mod n_1$. With our $\mod n_2$ glasses on, the equation is instead $x \equiv b_2 \cdot 1 + 0 = b_2 \mod n_2$.

[2] From Wikipedia: $https://en.wikipedia.org/wiki/Chinese_remainder_theorem$

Now that we have a method for finding x, we want to show that x is a unique solution to our system of congruences. So consider any integer of the form:

$$\begin{aligned}
&x' = x + kn_1n_2 \\
&x' = x + kn_1n_2 \equiv x \equiv b_1 && \mod n_1 \text{(Here we look at the entire row} && \mod n_1 \\
&x' = x + kn_1n_2 \equiv x \equiv b_2 && \mod n_2 \text{(Here we look at the entire row} && \mod n_2
\end{aligned}$$

$\therefore x'$ also solves the system of congruences we defined above as $\star$.

Now suppose x' is any solution to $\star$. We want to show that it is of this form:

$$\begin{aligned}
x' &\equiv b_1 \mod n_1 & \qquad x &\equiv b_1 \mod n_1 \\
x' &\equiv b_2 \mod n_2 & \qquad x &\equiv b_2 \mod n_2 \\
\therefore x' &\equiv x \mod n_1 & \qquad &\text{(From our rules for congruences)} \\
x' &\equiv x \mod n_2 &
\end{aligned}$$

It follows that $n_1|(x' - x)$ and $n_2|(x' - x)$
$\therefore n_1n_2|(x' - x)$ and $x' - x = kn_1n_2$ for some $k \in \mathbb{Z}$, which shows us that $x \equiv x' \mod n_1n_2$, so the solution is unique.

Inductive Hypothesis: Assume the above result holds true for all ℓ. **Inductive Step:** We will show the result holds true for $\ell + 1$.
Consider a system of the form:

$$\star\star = \begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ \vdots \\ x \equiv b_\ell \mod n_\ell \\ x \equiv b_{\ell+1} \mod n_{\ell+1} \end{cases} \quad \text{where any two } n_i \text{ are pairwise relatively prime.}$$

By the induction hypothesis, there is a solution x_0 to the first ℓ equations. Moreover, the full solution set to the first ℓ equations is

$$x_0 kn_1n_2 \dots n_\ell, k \in \mathbb{Z}, \text{ and define } N' = n_1n_2 \dots n_\ell$$

The full system $\star\star$ is then equivalent to the following pair of congruences:

$$\begin{cases} x \equiv x_0 \mod N' \\ x \equiv b_{\ell+1} \mod n_{\ell+1} \end{cases}$$

And we realize that $\gcd(N', n_{\ell+1}) = 1$, so this final system can be solved in exactly the same manner as we solved the basis step where $\ell = 2$. □

14.2 Examples

Example 15. Let's solve the first system we defined above:

$$\begin{cases} x \equiv 5 \mod 11 \\ x \equiv 7 \mod 13 \end{cases}$$

First we need to find α_1, α_2 such that we have a linear integer combination that satisfies Bezout's Theorem.

$$\alpha_1 11 + \alpha_2 13 = 1$$

$$\alpha_1 = 6, \alpha_2 = -5$$
$$6 \cdot 11 + (-5) \cdot 13 = 1$$

Now we use $x = b_2\alpha_1 n_1 + b_1\alpha_2 n_2$

$$x = 7 \cdot 6 \cdot 11 + 5 \cdot (-5) \cdot 13$$
$$x = 137$$

And note that $11 \cdot 13 = 143$, so a general solution is $137 + k143, k \in \mathbb{Z}$.

Example 16. What happens if we extend this to three equations? To make life easier on ourselves, let's just add an equation to the two we had above.

$$\begin{cases} x \equiv 5 \mod 11 \\ x \equiv 7 \mod 13 \\ x \equiv 4 \mod 6 \end{cases}$$

So we actually only need to solve:

$$\begin{cases} x \equiv 137 \mod 143 \\ x \equiv 4 \mod 6 \end{cases}$$

Using Bezout's theorem, we find a linear integer combination for $\gcd(6, 143) = 1$:

$$1 = 24 \cdot 6 + (-1) \cdot 143$$

So we have our α_1 and α_2. Next,

$$x_0 = 137 \cdot 24 \cdot 6 - 4 \cdot 1 \cdot 143$$
$$x_0 = 19156$$

And since $4 \cdot 143 = 858$, $x_0 = 19156 + k \cdot 858$ is the general solution.

15 Prime numbers

Here we are going to step back from congruences, algorithms and greatest common divisors to focus on one of the most interesting types of integers - prime numbers. Prime numbers show up in many places, and end up being incredibly useful in the study of cryptography. Incredibly useful is really an understatement - the entire edifice upon which modern public-key cryptography is built relies on our ability to discover and multiply large prime numbers together, and the ensuing difficulty in recovering those prime factors from the resultant composite product. But this is a digression, and we must return to our definitions before we can dig into the cryptography!

15.1 Definition of a prime number

definition 17. A positive integer p is *prime* if the only divisors of p are 1 and p itself.

15.2 Lemma on prime divisibility

Lemma 18. *If p is a prime and $p|ab$, then $p|a$ or $p|b$*

Proof. Our strategy for this proof is that we want to prove that if $p|ab$ and $p \nmid a$, then $p|b$.

Assume that $p \nmid a$. Since p is prime, this means that a and p are relatively prime, thus $\gcd(a, p) = 1$.
Using Bezout's Theorem, this tells us that $\exists s, t \in \mathbb{Z}$ such that $1 = as + pt$.
If we multiply both sides of the above equation, we get $b = s \cdot (ab) + b \cdot (pt)$
Since p divides the right side of this equation (the portion of each term on the right divisible by p is placed

in the parentheses), p also divides b.
$\therefore p|b$
We can show that $p|a$ by simply swapping a and b in the above proof, which is sufficient to prove the Lemma. This is known as **Euclid's Lemma**[3] □

Theorem 19. *Every $n \in \mathbb{N}$ with $n > 1$ has a factorization of the form:*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots p_l^{k_l}$$

Where $p_1, p_2, \ldots, p_l$ are distinct primes and $k_l > 0$

Proof. 19 We can prove this using strong induction.

1. *Basis step*: When $n = 2$, the result clearly holds, since 2 is prime.
2. *Inductive Hypothesis*: Suppose the result holds for $2, \ldots, n$ and we will show it holds for $n + 1$.
3. *Induction step*: If $n + 1$ is prime, we are done, as a prime number has a factorization of primes - itself. Otherwise, $n + 1$ is composite, thus $n + 1 = a \cdot b$ where $1 < a, b < n + 1$.
4. $\therefore$ both a and b have a factorization by primes from our Inductive Hypothesis, so $n + 1$ also has such a factorization.

□

Theorem 20. *The factorization in the previous theorem is unique up to a reordering of the primes $p_1, p_2, \ldots, p_l$.*

Proof. 20 We can also prove this using strong induction.

1. *Basis step*: When $n = 2$, the result holds, as there are no primes less than 2, which means that 2 cannot have an alternate factorization.
2. *Inductive Hypothesis*: Suppose the result holds for $2, \ldots, n$ and we will show it holds for $n + 1$.
3. *Induction step*: If $n + 1$ has two distinct factorizations, we would have:
   (*) $n + 1 = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots p_n^{k_n} = q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots q_m^{l_m}$
   Since $p_1|n + 1, \therefore p_1|q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots q_m^{l_m}$
   If $p_1 = q_i$ for any i, we could cancel p_1 from both sides of the equation we marked as (*). Then we would have an equation at a lower level and we could invoke the *inductive hypothesis* to say this is true.
   The other possibility is that $p_1 \neq q_i$ for all i. In this case, $\gcd(p_1, q_i) = 1 \; \forall i = 1, \ldots, m$
   By Lemma 13.2, we would then say:
   $p_1|q_1^{l_1 - 1} \cdot q_2^{l_2} \cdot \ldots q_m^{l_m}$ because we factored out the q_i that is relatively prime to p_1
   $p_1|q_2^{l_2} \cdot \ldots q_m^{l_m}$ and again, we factored out one of the q_i relatively prime to p_1
   $\vdots$ We repeat this factoring out of q_i relatively prime to p_1 until we get
   $p_1|1$ Which is clearly a contradiction.
4. $\therefore p_1 = q_i$ for some i, and the factorization is unique up to reordering of the prime factors.

□

[3] William Stein, Elementary Number Theory, Theorem 1.1.19, p.7 (http://wstein.org/ent/ent.pdf)

15.3 There are Infinitely Many Prime Numbers

15.3.1 Theorem (Euclid)

Proof. By Contradiction - Suppose there are only finitely many primes.
List all of the primes: $p_1, p_2, \ldots, p_n$
Set $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$
m **must** have a prime factorization, since $m \geq 2$
$\therefore m$ has a prime factor q, and $q = p_i$ for some $i = 1, \ldots, m$
We can factor this q out of m, which gives us $m = q(p_1 \cdot \ldots \cdot \hat{p_i} \cdot \ldots p_n) + 1$, where $\hat{p_i}$ represents the p_i we factored out as q. However, this immediately presents us with a contradiction, since we have assumed q is a factor of m, but we see that $q \nmid m$, because the remainder upon division by q is 1.
$\therefore$ There are infinitely many prime numbers. □

16 Euler totient function

Now that we have some good feelings about prime numbers, let's move on and examine some useful functions that will help us in working with prime numbers and congruences.

definition 21. The Euler totient function, written as $\phi(n)$, counts the number of invertible elements in $\mathbb{Z}_n$. Recall that an element of $\mathbb{Z}_n$ is invertible if it is relatively prime to n, so it is equivalent to say that $\phi(n)$ counts the number of elements in the list $\{0, 1, 2, \ldots, n-1\}$ that are relatively prime to n.
Formally we would state:

$$\phi(n) = \#(a : 0 \leq a < n \text{ and } \gcd(a, n) = 1)^4$$

16.1 Examples of $\phi(n)$

As stated above, $\phi(n)$ is simply the number of integers from 0 to $n-1$ which are relatively prime to n. We can state this for several small integers.

- $\phi(5) = \#\{1, 2, 3, 4\} = 4$
- $\phi(8) = \#\{1, 3, 5, 7\} = 4$
- $\phi(24) = \#\{1, 5, 7, 11, 13, 17, 19, 23\} = 8$

16.2 If p is prime, $\phi(p) = p - 1$

The proof of this is simply a counting exercise derived from the definition of the Euler ϕ function. Since every number from 1 to $p-1$ is relatively prime to p when p is a prime number, and there are $p-1$ numbers in that list, then 14.2 directly follows from those facts.

16.3 Euler phi function of prime powers: $\phi(p^n)$

Theorem 22. *If p is prime and n is a positive integer, then $\phi(p^n)$ has the following value:*

$$\phi(p^n) = p^n - p^{n-1}$$

Proof. [5] $\phi(p^n)$ is defined as all of the integers in the list $\{0, 1, 2, \ldots, p^n - 1\}$ which are relatively prime to p^n. Since p is prime, it will be relatively prime with any element of this list except for those with a factor of p - which will be those p^a where $a < n$. Which gives us:

$$\phi(p^n) = p^n - \frac{p^n}{p} \qquad (p^n \text{ minus the number of elements divisible by } p)$$

$$\phi(p^n) = p^n - p^{n-1} \qquad \text{(And simplifying the exponent gives us our formula)}$$

[4] http://people.emich.edu/jramanath/docs/math409-592w17/elemNumTh02.pdf - Slide 15
[5] Stein, result 2.2.2, page 27

□

16.4 Euler phi function of composite numbers: $\phi(n)$

Theorem 23. *If n_1, n_2 are positive, relatively prime integers, then:*

$$\phi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2)$$

Proof. Consider the following function:

$$F : \mathbb{Z}_{n_1 n_2} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

Defined by $F(x) = (x \mod n_1, x \mod n_2)$. Notice that since we're operating with our congruence glasses on, the value of F is not going to change when we shift by multiples of $n_1 n_2$.
Next, suppose that x is a unit in $\mathbb{Z}_{n_1 n_2}$. Then $\gcd(x, n_1 n_2) = 1$ and Bezout's Theorem tells us that there are integers u, v such that $xu + n_1 n_2 v = 1$. Furthermore, this implies that:

$$xu = 1 \mod n_1$$
$$xu = 1 \mod n_2$$

$\therefore F(x) \in \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$, where $\mathbb{Z}_n^*$ is the group of units in $\mathbb{Z}_n$. Now, let's consider restriction the definition of F to $\mathbb{Z}_{n_1 n_2}^*$:

$$F : \mathbb{Z}_{n_1 n_2}^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$$

And we claim that F is bijective. To prove that there is a bijection, we must prove injectivity and surjectivity.

Injectivity: To prove injectivity we want to show that every element in the range of F maps to a unique element in the domain. That is, we want to show that if $F(x) = F(x')$, then $x = x'$.
To begin, suppose $F(x) = F(x')$. This means that:

$$x \mod n_1 = x' \mod n_1$$
$$x \mod n_2 = x' \mod n_2$$

Which is equivalent to

$$x' - x \equiv 0 mod n_1$$
$$x' - x \equiv 0 mod n_2$$

So we have $n_1 | x' - x$ and $n_2 | x' - x$. Since $\gcd(n_1, n_) = 1$, then from our rules about relatively prime numbers and divisibility we have $n_1 \cdot n_2 | x' - x$.
$\therefore x' \mod (n_1 n_2) = x \mod (n_1 n_2)$, which shows that F is injective.

Surjectivity: To prove that there is a surjection, we want to show that for any $a \mod n_1$ that is a unit in $\mathbb{Z}_{n_1}$ and $b \mod n_2$ that is a unit in $\mathbb{Z}_{n_2}$ there exists some x such that

$$x \equiv a \mod n_1$$
$$x \equiv b \mod n_2$$

Technically, if we can show this then we have shown that the range and domain of our function F are the same size, which is sufficient to prove surjection. Now, the above two congruences should look familiar - we know that we can find an x that satisfies both equations using the Chinese Remainder Theorem. Further, the solution is unique modulo $n_1 n_2$, which is what we need. Specifically, the solution is given by:

$$F(x \mod n_1 n_2) = (a \mod n_1, b \mod n_2)$$

Which tells us that the sets $\mathbb{Z}_{n_1 n_2}$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ have the same size.

$$\begin{aligned} \therefore \phi(n_1 n_2) &= \#(\mathbb{Z}_{n_1 n_2}) \\ &= \#(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}) = \phi(n_1) \cdot \phi(n_2) \end{aligned}$$

□

16.4.1 Examples

Above we showed that $\phi(8) = 4$, and $\phi(24) = 8$ by counting out the relatively prime integers. Now let's use our new theorems to do the calculations.

- $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$
- $\phi(24) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^2) \cdot (3 - 1) = 4 \cdot 2 = 8$
- $\phi(91) = \phi(13) \cdot \phi(7) = 12 \cdot 6 = 72$

17 Fermat's Little Theorem

Theorem 24. *Let p be a prime, and $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Then we have*

$$a^{p-1} \equiv 1 \mod p$$

Proof. Define $F : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ by $F(x) = ax \mod p$
Suppose that $F(x) = F(x')$ this directly implies that $ax \equiv ax' \mod p$. We know that a is invertible, so let α be the inverse of $a \mod p$. Then we can multiply both sides by α to get

$$(\alpha a)x \equiv (\alpha a)x' \mod p$$

$$\therefore x \equiv x' \mod p$$

$\therefore F$ is injective, and since the domain and range are the same size (and finite), injectivity implies surjectivity. So F is a bijection, and we can say that the list

$$1 \mod p, 2 \mod p, \ldots (p-1) \mod p$$

and the list

$$1 \cdot a \mod p, 2 \cdot a \mod p, \ldots, (p-1) \cdot a \mod p$$

are the same, ignoring reordering (they are permutations of each other).
$\therefore (p-1)! \equiv a^{p-1} \cdot (p-1)! \mod p$
And since $(p-1)! \mod p$ is invertible, we can cancel it from both sides of the equation, which gives us:

$$1 \equiv a^{p-1} mod p$$

□

17.1 Pseudoprimes

Pseudoprimes are not prime numbers, but they have some useful properties. Fermat's Little Theorem gives us a method for discovering pseudoprimes. We define an integer $n > 1$ as being pseudoprime relative to a if $\gcd(a, n) = 1$ and

$$a^n \equiv a \mod n$$

17.2 Using Fermat's Little Theorem to do computations

Fermat's Little Theorem gives us a way to reduce exponents in a given modulus, which allows us to calculate large exponents modulo a specific p very easily. We'll do an example.

Example 25. Calculate $14^{2004} \mod 23$ using Fermat's Little Theorem.

1. Fermat's Little theorem states that if $x \not\equiv 0 \mod 23$, then $x^{22} \equiv 1 \mod 23$
2. Clearly $14 \not\equiv 0 \mod 23$

3. So we use the division algorithm to find $2004 = 22q + 2$,
4. Next we break down our original equation: $(14^{22})^q \cdot 14^2 \mod 23$
5. Using Fermat's Little Theorem we see that $(14^{22})^q \equiv 1 \mod 23$
6. So we can write $1 \cdot 14^2 \mod 23$
7. Which is simply $196 mod 23 = 12$

18 Euler's Theorem

Theorem 26. *Let $n > 1$ be a given integer, and suppose $a \in \mathbb{Z}$ satisfies $\gcd(a, n) = 1$ (That is, a and n are relatively prime.) Then:*

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

Proof. Let's define $\star = \{u_1, u_2, \ldots, u_{\phi(n)}\}$ as a listing of the integers in the list $\{1, 2, \ldots, n\}$ which are relatively prime to n.
Now, define for $i = 1, \ldots, \phi(n)$: v_i as the remainder of $a \cdot u_i$ upon division by n.
Note that each v_i is in the list $\star$. Moreover:

$$\begin{aligned} v_i &\equiv v_j \mod n \\ \Rightarrow au_i &\equiv au_j \mod n \\ \Rightarrow u_i &\equiv u_j \mod n && \text{(Since a is invertible)} \\ \Rightarrow i &= j \end{aligned}$$

$\therefore v_1, v_2, \ldots, v_{\phi(n)}$ is just a rearrangement of $u_1, u_2, \ldots, u_{\phi(n)}$
So we can further write:

$$\begin{aligned} u_1, u_2, \ldots, u_{\phi(n)} &\equiv v_1, v_2, \ldots, v_{\phi(n)} \mod n \\ u_1, u_2, \ldots, u_{\phi(n)} &\equiv (au_1), (au_2), \ldots, (au_{\phi(n)}) \mod n \\ u_1, u_2, \ldots, u_{\phi(n)} &\equiv a^{\phi(n)}(u_1, u_2, \ldots, u_{\phi(n)}) \mod n \end{aligned}$$

And since $u_1, u_2, \ldots, u_{\phi(n)} \mod n$ is invertible, we can cancel it from both sides and get

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

□

18.1 Using Euler's Theorem to do computations

Euler's Theorem also gives us a way to reduce exponents in a given modulus. While Fermat's Little Theorem can only be used when the base of the exponent is not congruent to $0 \mod p$, Euler's Theorem is slightly more general, and can be used whenever the base of the exponent is a unit in the given modulus. So we can use Euler's Theorem in non-prime modulus classes.

Example 27. Calculate $13^{2017} \mod 24$ using Euler's Theorem

1. Euler's theorem works if $x \mod 24$ is a unit, and $\gcd(13, 24) = 1$, so 13 is a unit.
2. We need to calculate $\phi(24) = 8$, which we did earlier (see example 16.4.1)
3. So we use the division algorithm to find $2017 = 8q + 1$,
4. Next we break down our original equation: $(13^8)^q \cdot 13^1 \mod 24$
5. Using Euler's we know that $(13^8)^q \equiv 1 \mod 24$
6. So we can write $1 \cdot 13^1 \mod 24$
7. Which is simply $13 \mod 24 = 13$

19 Algorithms

Number Theory allows us to discover some useful algorithms. Here are a few of them. In general I'm going to gloss over any descriptions of pseudocode or even specific code, since I'm far more comfortable writing code than writing proofs.

19.1 Fast multiplication mod p

definition 28. Fix some $n \geq 1$. We can computer $a^k \mod n$, where $a \in \mathbb{Z}$ and k is a positive integer.
We expand p in terms of its binary representation:

$$k = b_0 \cdot 2^0 + b_1 c\dot{2}^1 + b_2 \cdot 2^2 + \ldots + b_\ell \cdot 2^\ell$$

Where $b_i = 0$ or 1 for $i = 0, \ldots, \ell$. And the binary expansion of k is thus written: $b_\ell b_{\ell-1} b_{\ell-2} \ldots b_0$, where b_0 is the least significant bit. In terms of a^k, this gives us:

$$\begin{aligned} a^k &= a^{b_0 \cdot 2^0 + b_1 c\dot{2}^1 + b_2 \cdot 2^2 + \ldots + b_\ell \cdot 2^\ell} \\ &= a^{b_0 \cdot 2^0} \cdot a^{b_1 c\dot{2}^1} \cdot a^{b_2 \cdot 2^2} \cdot \ldots \cdot a^{b_\ell \cdot 2^\ell} \\ &= a^{b_0} \cdot (a^2)^{b_1} \cdot (a^4)^{b_2} \cdot \ldots \cdot (a^{2^\ell})^{b_\ell} \end{aligned}$$

Which we can use to compute the exponent $\mod k$.

19.2 Example

Let $a = 7$, $k = 151$, $n = 11$, and find $a^k \mod n$. So find $7^1 51 \mod 11$.
The binary representation of 151 is 10010111_2 We start with the least significant bit, calculate $a^{b_i} \mod n$ for each bit, and multiplying the result by the value in the accumulator $\mod n$ if the bit of k is 1. If the bit is not 1, we do the calculation anyway but skip storing the result to the accumulator.

bits of p	powers of $a \mod n$	Accumulator $\mod n$
1	$a^{b_0} = 7 \mod 11 = 7$	7
1	$(a^2)^{b_1} = 49 \mod 11 = 5$	$(35 \cdot 7) \mod 11 = 2$
1	$5^2 \mod 11 = 3$	$(3 \cdot 2) \mod 11 = 6$
0	$3^2 \mod 11 = 9$	bit is zero, skip
1	$9^2 \mod 11 = 4$	$(4 \cdot 6) \mod 11 = 2$
0	$4^2 \mod 11 = 5$	bit is zero, skip
0	$5^2 \mod 11 = 3$	bit is zero, skip
1	$3^2 \mod 11 = 9$	$(9 \cdot 2) \mod 11 = 7$

$\therefore 7^1 51 \mod 11 = 7$

20 Algorithm - Fast Sieve of Eratosthenes

The Sieve of Eratosthenes is a prime number sieve that provides a simple method for finding prime numbers up to some integer n. The general way that the sieve works is that it creates a list of all integers up to n, then starting at 2, it removes all multiples of 2 from the list. Then it finds the next prime (3), and removes all multiples of three from the list. It continues on until it reach n. At least, that's the standard method. The fast method only goes up to$\sqrt{n}$.

Lemma 29. *If n is composite, then it has a proper divisor a such that $a \leq \sqrt{n}$*

Proof. Suppose n is composite. Then there are positive integers x, y such that $n = x \cdot y$, and $1 < x, y < n$. Consider the situation where both x and x are greater than $\sqrt{n}$. Then

$$n = x \cdot y > \sqrt{n} \cdot \sqrt{n} = n$$

Which is a contradiction, since n is clearly not greater than itself. So at least one of x or y must be no greater than $\sqrt{n}$. □

20.1 Python code to implement the fast sieve

Since I've never implemented this before taking Cryptography, here's an implementation in Python:

```
In [1]: from math import sqrt

        def fastErat(n):
                """ Fast version of the sieve of Eratosthenes. Only multiple
                of primes up to sqrt of n are filtered."""
                #print(2)
                primes = []
                if n < 2: return(primes)
                testbnd = sqrt(n + 0.000001)
                nxtpr = 1
                lst = [x for x in range(2,n+1)]
                while (lst != []) and (nxtpr <= testbnd) :
                        nxtpr = lst[0]
                        primes.append(nxtpr)
                        lst = [x for x in lst if (x%nxtpr) != 0]
                return(primes+lst)
```

21 Algorithm for fast GCD computation using bit shift operations

We can use our GCD identities combined with the bit shift operations to implement a fast method of computing the GCD. Fast in the sense that the division algorithm can be expensive for large numbers, but a bit shift works in constant time.

21.1 Python code to implement bit-shift GCD

```
In [1]: def mygcd(a,b):
            x = abs(a)
            y = abs(b)
            g = 1
            #print('Computing the gcd of {0} and {1}'.format(x,y))
            while min(x,y) > 0:
                rx = x & 1                  # rx = x mod 2
                ry = y & 1                  # ry = y mod 2
                if (rx == 0 and ry == 1):
                    x = x >> 1              # x = x/2
                elif (ry == 0 and rx == 1):
                    y = y >> 1              # y = y/1
                elif (rx == 0 and ry == 0):
                    g,x,y = 2*g,x>>1,y>>1
                else:
                    x,y = abs(y-x),min(x,y)

            return max(x,y) * g
```