Cryptology and the Power of Primes

Purpose

The end goal of this lesson is to bring students who have a basic understanding of number theory, concepts of divisibility, prime factorization, and modular arithmetic, to the foundations of cryptology. I've chosen a (very simplified) version RSA cryptosystem for this role because of its prevalence in communications and its elegance. Euler's totient function φ and the Fermat-Euler Theorem are necessary prerequisites for understanding the beauty of this system (and cryptology in general), so their derivations are included as well. Additionally, there are some rather neat party tricks that we've compiled to scare away your 'friends' with. Finally, the order in which material is written here may not be the order in which it is presented (i.e we may elect to summarize or skip entire sections).

Part 0: Conventions & Assumptions

Definition 1: A number, a , is relatively prime to another number, b iff $\gcd(a, b) = 1$. In other words, a and b share no (prime) factors.

Definition 2: The totient function, $\varphi(n)$, returns the number of integers less than or equal to n which are relatively prime to it. For example, $\varphi(6) = 1$ because there is only 1 number less than 6 (namely, 5 as we do <u>not</u> include 1) that is relatively prime to 6. Additionally, this function is multiplicative, meaning $\varphi(ab) = \varphi(a)\varphi(b)$ for relatively prime a and b .

Definition 3: The number of elements that inhabit a set is its <u>cardinality</u>. For example, the cardinality of $S = \{0,1,2,3\}$ is $|S| = 4$.

Structure 1: The modulo structure, generally $a \equiv b\ (mod\ c)$ implies that $a = cq + b$, where $a, b, c, q \in \mathbb{Z}$. Although division doesn't usually "work" across the modulo, we have that $aqx \equiv bq\ (mod\ c)\ \Rightarrow\ ax \equiv b\ (mod\ c)$ if q and c are coprime. (In other words, we can divide both sides by a factor that is relatively prime to the modulo).

Structure 2: An inductive proof is a discrete structure used to prove a conjecture over $\mathbb{Z}^{+}$. If we prove the statement on some base case, assume it at an arbitrary value, and show that it holds for the next, we will have proved the statement over its domain. We will discuss a specific example later!

Part 1, p-Factors and Mods: Number Theory Basics

There are many ways of describing numbers; their position with respect to each other, with respect to 0, with respects to multiples, squares, cubes etc. We will study two methods

1. Prime factorization, the division of a number as the product of indivisible (prime) numbers. For example, we can break down 60 into $2^2 \cdot 3 \cdot 5$ and 2730 as $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. The Fundamental Theorem of Arithmetic guarantees that a given number n has a prime factorization that is unique.
2. The Greatest Common Divisor, which is a function that “takes in” two numbers and returns the largest number that divides them both. This number may be calculated by taking the largest degree of each shared prime. For example,

   $$\gcd(60,\ 2730) = \gcd(2^2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13) = 2^1 \cdot 3 \cdot 5 \cdot 7^0 \cdot 13^0 = 30.$$

   In addition, we may use the Euclidean Algorithm to find the same result, which simplifies our problem to the greatest common divisor between the smaller number and the remainder when the larger number is divided by the smaller one. This procedure continues all the way until the “result” is 0, at which point the other number is the desired greatest common divisor. This is what’s called a “recursive algorithm” and, in the spirit of computation, here is a pseudocode of all those words:

   ```
   int function gcd(int A,int B)
           if (A=0): return B
           if (B=0): return A
           else if (A>B): return gcd(A%B, B) //A%B is remainder of A/B
           else if (B>A): return gcd(A, B%A)
   ```

   If the greatest common divisor of two numbers is one, we call them “relatively prime” or “coprime” because they share no common factor. It can be shown that

   $$\gcd(a,b) = 1 \Rightarrow ax + by = 1 \text{ for } x,y \in \mathbb{Z}\ .$$

Now, we’ll study Structure 1, the ‘mod’ in more depth. From our structure definition in the intro, we find that b is essentially the “remainder” when a is divided by c . For example, $17 \equiv 3\ (mod\ 7)$, read as “17 is congruent to 3, modulo 7”, because $17 = 2 \cdot 7 + 3$. Therefore, by the nature of division and remainders, when a modular expression is in simplest form, we have $0 \leq b < c$.

Additionally, we can add or subtract as many c ‘s as we like to either side of the expression independently. For example, we could say

$$17 \equiv 3 \Rightarrow 17 + 3 \cdot 7 \equiv 3 - 2 \cdot 7 \Rightarrow 38 \equiv -11\ (mod\ 7).$$

Although this isn’t exactly in simplest form, this format is indeed equivalent and can often be useful, as we’ll see in this next case. Let’s say you wanted to solve a modular congruency of the form $ax \equiv b\ (mod\ c)$, like

$$2x \equiv 4 \ (mod\ 6).$$

One might be tempted to "divide by 2" and achieve $x \equiv 2\ (mod\ 6)$ and call it a day. However, by doing so, we miss out on a solution like $x = 5$; $2 \cdot 5 = 10 \equiv 4\ (mod\ 6)$, but $5 \neq 6k + 2$. What happened? It turns out that, for most cases, we are not allowed to "divide" both sides of a modular equation.

Now let's consider another congruency,

$$3x \equiv 5\ (mod\ 10).$$

Obviously, we can't divide by 3, because $x \equiv 5/3\ (mod\ 10)$ is nonsensical (how can we get a remainder of 5/3 when dividing by 10?). To solve this, we multiply by 3's "modular inverse," represented by $3^{-1}\ (mod\ 10)$, which has the property that $3 \cdot 3^{-1} \equiv 1\ (mod\ 10)$, just as we'd expect from an inverse! Of course, we'd like this inverse to be between 0 and 9 so its more tangible. Through some casework, we find that $3^{-1}\ (mod\ 10) = 7$ because $3 \cdot 7 \equiv 1\ (mod\ 10)$. Applying this inverse to the equation, we have

$$3x \equiv 5\ \Rightarrow 7 \cdot 3x \equiv 7 \cdot 5 \Rightarrow x \equiv 35 \Rightarrow x \equiv 5\ (mod\ 10),$$

which is easily verifiable.

It turns out that $a^{-1}\ (mod\ c)$ exists iff $\gcd(a, c) = 1$. In cases where both a divides both b and c , and $\gcd(a, c) = 1$ multiplying by a^{-1} is apparently equivalent to "dividing both sides" by a , and, in such cases, we will treat it as such.

Part 2: The Totient Function

We will attempt to write $\varphi(n)$ in closed form for all n . (Definition 2)

Derivation: For this daunting task, we will divide our problem into k subproblems – a very useful strategy! By the Fundamental Theorem of Arithmetic, we know that we can prime factorize $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. By definition, all of our primes are relatively prime, so

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \ldots \varphi(p_k^{e_k}).$$

Now, we must find the totient function for a number with only <u>one</u> prime factor, which is repeated. In other words, we must find how many numbers in the set

$$S = \{1,2,3 \ldots p^e\}$$

that are <u>not</u> divided by p . (Note: If a number is not divisible by p , it is relatively prime to p^e by definition, because it doesn't share the only prime factor.) Trivially, we have $|S| = p^e$.

Suddenly our number theory endeavor has turned into a counting exercise! Tipped off by the word “not,” we suspect using complementary counting will be successful. So, we will find the number of elements in S that are divided by p . These are just the multiples of p or

$$D = \{p, 2p, 3p \dots p^e\}.$$

By comparing D to a set where each element is $1/p$ as large, namely $D_{1/p} = \{1,2,3 \dots p^{e-1}\}$, we find that $|D| = |D_{1/p}| = p^{e-1}$. Therefore, our complement, the number of relatively prime integers is

$$\varphi(p^e) = |S| - |D| = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right).$$

Now, returning from our k subproblems to our initial quantity, and strategically rearranging we have:

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2})\dots\varphi(p_k^{e_k}) = p_1^{e_1}\left(1 - \frac{1}{p_1}\right)p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\dots p_k^{e_k}\left(1 - \frac{1}{p_k}\right)\\ &= (p_1^{e_1}p_2^{e_2}\dots p_k^{e_k})\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)\\ &= (p_1^{e_1}p_2^{e_2}\dots p_k^{e_k})\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right). \quad \blacksquare\end{aligned}$$

For a sanity check, let’s plug in any prime number p ,

$$\varphi(p) = p\left(1 - \frac{1}{p}\right) = p - 1.$$

This matches with our expectations, as, from the list $\{1,2,3, \dots p\}$ only p isn’t relatively prime.

From this proof, we note a seemingly trivial yet essential property:

Property 1a:

The maximum cardinality of the set of $\mathbb{Z}^+$less than n and coprime to it is $\varphi(n)$, and this set is unique.

Property 1b (Converse):

If we have a set with elements in $\mathbb{Z}^+$ of cardinality $\varphi(n)$ with each element smaller than and coprime to n , the set is unique and of maximum length.

*Part 3: Fermat’s Little Theorem**

We will prove that $a^p \equiv a \ (mod\ p)$, where p and a are coprime (relatively prime).

Proof: We will prove this by induction, beginning with a base case. It makes sense to begin with $a = 1$, and it is trivial to show that

$$1^p \equiv 1\ (mod\, p).$$

Now for the leap! We will assume that $a^p \equiv a\ (mod\, p)$, and would like to show that $(a+1)^p \equiv a+1\ (mod\, p)$. To do so, we will begin expanding the LHS using the binomial theorem.

$$(a+1)^p \equiv a^p + pa^{p-1} + \frac{p(p-1)}{2}a^{p-2} + \cdots + pa + 1\ (mod\, p).$$

Although this may initially seem messy, notice that every term in the expansion except for the first and last term is divisible by p and is therefore congruent to 0 modulo p !! We also know, from our assumed statement that our first term is just congruent to a modulo p. Finally, our statement reduces to

$$(a+1)^p \equiv a + 0 + 0 + \cdots + 0 + 1 \equiv a + 1\ (mod\, p),$$

completing our proof! ■

Part 4, putting it all together: the Fermat-Euler Theorem

We will prove a generalization of part 2, using the totient function: $a^{\varphi(n)} \equiv 1\ (mod\, n)$ with coprime n and a .

Proof: Consider the sets

$$S_1 = \{x_1, x_2, x_3, \dots x_{\varphi(n)}\} \text{ and}$$

$$S_2 = \{ax_1, ax_2, ax_3, \dots ax_{\varphi(n)}\}\ (mod\, n).$$

where $x_i < n$, $\gcd(x_i, n) = 1$, and $\gcd(a, n) = 1$ for $1 \leq i \leq \varphi(n)$.

Using Property 1a, we immediately recognize S_1 as the unique set of $\varphi(n)$ integers smaller than n with no shared factors.

Now we will consider S_2. When we completely simplify all $ax_i\ (mod\, n)$, the result must be less than n . Additionally, since neither a nor x_i share common factors with n , we have that ax_i doesn't either! Therefore, S_2 is a set of cardinality $\varphi(n)$, each element less than n and relatively prime to it. So, by Property 1b, we have that S_2 is also the unique set of smaller, coprime integers!

How can this be? S_1 and S_2 look nothing alike yet our theorems state that they contain identical elements! It's important to notice that the i^{th} element of S_1 is not necessarily shared with the i^{th} in S_2, rather the contents are equivalent, just in a scrambled order.

Now for the strategic part of the proof. Since we have just shown the sets are equivalent modulo n , the product of each element in each set must be equivalent. Therefore,

$$x_1x_2x_3\ldots x_{\varphi(n)} \equiv ax_1ax_2ax_3\ldots ax_{\varphi(n)} \ (mod\ n)$$
$$\Rightarrow x_1x_2x_3\ldots x_{\varphi(n)} \equiv a^{\varphi(n)}x_1x_2x_3\ldots x_{\varphi(n)} \ (mod\ n).$$

Since that huge product $x_1x_2x_3 \ldots x_{\varphi(n)}$ is coprime to n , we can happily divide it away, resulting in $a^{\varphi(n)} \equiv 1 \ (mod\, n)$ and completing our proof! ■

Remembering that $\varphi(n) = n - 1$ iff n is prime, we have that $a^{n-1} \equiv 1 \ \Rightarrow a^n \equiv a \ (mod\, n)$immediately for prime n . Fermat's Little Theorem is just a super-special case of this broader concept!

*Part 5: Nifty Party Tricks!**

5.1: What is the hundred's digit of $7^{402} + 3^{1199}$?

Solution: The last 3 digits of that hideous sum is just $7^{402} + 3^{1199} \ (mod\, 1000)$ will reveal the hundred's place, so we must first find this value. Note that

$$\varphi(1000) = 1000\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{5}\right) = 400.$$

Conveniently, 7's exponent is near $\varphi(1000)$, so $7^{402} \equiv (7^{400})(7^2) \equiv 1 \cdot 49 \ (mod\, 1000)$.

However, 3's exponent is a little trickier. We know

$$3^{1200} \equiv (3^{400})^3 \equiv 1^3 \equiv 1 \ (mod\, 1000).$$

So, if we set $x \equiv 3^{1199} \ (mod\, 1000)$, we have

$$3x \equiv 1 (mod\, 1000).$$

We notice that 3 divides $2 \cdot 1000 + 1 = 2001$, so $x \equiv 3^{1199} \equiv 667 \ (mod\, 1000)$.

At last, we have $7^{402} + 3^{1199} \equiv 49 + 667 \equiv 716 \ (mod\, 1000)$, so, our hundred's digit is 7. ■

5.2: Find the least odd prime factor of $2019^8 + 1$. (AIME)

Solution: We desire the smallest possible prime p where $2019^8 \equiv -1 \ (mod\, p)$. Since we can use so many tools when the RHS is 1, we square our given equation to

$$2019^{16} \equiv 1 \ (mod\, p).$$

We're familiar with this form from Fermat's Little Theorem! The exponent, 16, must be some multiple of $p-1$ because we know $2019^{p-1} \equiv 1\ (mod\ p)$. So, $p \equiv 1\ (mod\ 16)$ (Note: We can't just call it quits and claim $p = 16 + 1 = 17$ because our exponent may have been a square root or cube root etc. of the true $p-1$. We must test all, or at least the first few, multiples of 16). We will now break into casework checking primes that are 1 over a multiple of 16:

<u>Case 1</u>, $p = 16 \cdot 1 + 1 = 17$:

Through brute force, we find $2019 \equiv 13\ (mod\ 17)$ so $2019^2 \equiv 13^2 \equiv -1\ (mod\ 17)$. Then, $2019^8 \equiv 1 \neq -1\ (mod\ 17)$, so, this case fails. 🙁

<u>Case 2</u>, $p = 16 \cdot 6 + 1 = 97$:

By more brute force, we discover

$$2019 \equiv -18\ (mod\ 97),$$

$$2019^2 \equiv (-18)^2 \equiv 324 \equiv 33\ (mod\ 97),$$

$$2019^4 \equiv 33^2 \equiv 1089 \equiv 22\ (mod\ 97),$$

$$2019^8 \equiv 22^2 \equiv 484 \equiv -1\ (mod\ 97).$$

Success! Using $p = 97$ satisfies our initial condition for the first time and we thank our lucky stars for no more cases. ■

(The prime factorization of $2019^8 + 1$ is $2 \cdot 97 \cdot 1423275002072658812388593$, including a VERY large prime number!)

Part 6, large primes?!: The Rivest-Shamir-Adleman (RSA) Cryptosystem

Encryption deals with passing information between endpoints such that, if intercepted, the message is impossible or very difficult to decipher. In the RSA system, each party has a public key, which is known to everyone, and a private key, which is kept in secret. For example, if Alice wanted to send Bob a message, she would use Bob's public key (which is available to everyone) to encrypt her message. Upon receiving this cipher, Bob would then use his private key to decode the message.

The Idea

Let's say that Alice wants to send a message which she has numerically translated to m (for simplicity, let's say this is ASCII). In the RSA system, Bob must release a public key (n, e) to Alice but he withholds a specially designed private key d where $m, n, e, d \in \mathbb{Z}^+$ and $0 \leq m < n$ (though all are very large).

In the RSA system, Alice would refer to Bob's keys and send the message $m^e\ (mod\ n)$ to Bob, which he would decipher back to m by exponentiating his unique private key!

$$(m^e)^d \equiv m\ (mod\ n).$$

Before we continue with the math, try to "break" this code yourself! Let's say that Charles is snooping in on this conversation – he can see every bit that is transferred between Alice and Bob. He captures Alice's message of $m^e\ (mod\ n)$ and has knowledge of Bob's public keys (n, e), but he's utterly lost on how to convert this mess back to m !

The Method

1. Choose two distinct (and large) prime numbers p and q . The primes should be similar in size (just a couple digits apart) and greater than the actual message m .
2. Calculate $n = pq$.
3. Choose an integer $e \in \big(1, \varphi(pq)\big)$ such that $\gcd\big(e, \varphi(n)\big) = 1$ (they are coprime).
    a. This (n, e) will be released as the public key.
4. Determine d as $de \equiv 1\ \big(mod\ \varphi(n)\big)$. d is the modular inverse of e modulo $\varphi(n)$. Since e and $\varphi(n)$ are coprime, d exists uniquely.

Well, thanks to step 4, d doesn't seem all that private anymore! All Charles has to do is find the modular inverse of e modulo $\varphi(n)$! He has already intercepted that from Bob, so it seems it would just take some bashing. However, although we may know n , $\varphi(n)$ is a different story. Recall that, since $n = pq$, $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. So, unless we can actually prime factorize n , which is difficult due to the sheer size of the primes, we don't actually know anything about $\varphi(n)$ and our secret key is extra safe.

It's incredible that these 3 simple steps produce one of the strongest ciphers ever created. Charles knows every detail between Alice and Bob, the public keys, the message, even the method in which the private key is created! He's so tantalizingly close to breaking the code, but without that difficult prime factorization it's impossible!

The Proof

Now, we will show the RSA encryption is a little less than magic by showing that, for our selected (m, n, e, d) the statement $(m^e)^d \equiv m\ (mod\ n)$ holds. If we can show this, Alice will have successfully encrypted her message, Bob will have decrypted it, and Charles will be wailing in agony.

Since $ed \equiv 1\ \big(mod\ \varphi(n)\big)$ by definition, we have $ed = k\varphi(n) + 1$ for some $k \in \mathbb{Z}^+$. Therefore,

$$(m^e)^d \equiv m^{ed} \equiv m^{k\varphi(n)}m\ (mod\ n).$$

Since $m < p, q$, we have that $\gcd(m, n) = 1$ because they share no (prime) factors. So, our conditions are met and we are now allowed to apply the Fermat-Euler Theorem.

$$m^{k\varphi(n)}m \equiv \left(m^{\varphi(n)}\right)^k m \equiv 1^k m \equiv m \ (mod\, n)$$

which completes our proof. ■

Summary

- For a modular statement $ax \equiv b \ (mod\ c)$, we have $ax = cq + b$ for some $q \in \mathbb{Z}$. If $\gcd(a, c) = 1$ (they are relatively prime) we have the following properties:
    - $ax \equiv b \ (mod\ c) \Rightarrow x \equiv b/a \ (mod\ c)$ if a divides b .
    - $ax \equiv b \ (mod\ c) \Rightarrow x \equiv a^{-1}b \ (mod\ c)$ where $a^{-1}a \ \equiv 1 \ (mod\ c)$ and $0 \leq a^{-1} < c$ (some unique a^{-1} will always exist under these conditions).
- Euler's Totient function states that, for any integer $n = p_1^{e_1}p_2^{e_2} \dots p_k^{e_k}$, the number of positive integers less than it is

$$\varphi(n) = \prod_{i=1}^{k} n\left(1 - \frac{1}{p_i}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

    - ⇔ There are $\varphi(n)$ less than n that are relatively prime to it (coprime, $\gcd$ w/ n is 1, etc.).
    - ⇔ If we find a set of $\varphi(n)$ integers less than n that are all relatively prime to it, the set is <u>unique.</u>
- The Euler-Fermat Theorem states that

$$a^{\varphi(n)} \equiv a \ (mod\, n)$$

  for relatively prime a and n .

    - A special case of this theorem, called Fermat's Little Theorem, states that

$$a^{p-1} \equiv a \ (mod\, p)$$

  for coprime a and p .

- The RSA Cryptosystem allows for private, encrypted communication to be breached however the information is difficult to retrieve.
    - To send a message m , the sender must know both of the recipients public keys, (n, e), while withholding (never sending) a private key d . The sender will encrypt the message by sending $m^e \ (mod\, n)$.
    - The recipient decrypts this message by exponentiating it with his private key, finding $(m^e)^d \ (mod\, n)$ which can be shown to be equivalent to $m \ (mod\, n)$.
    - Conditions: $n = pq$ where p and q are prime numbers (usually around $2^{4096} \approx 10^{400}$ in the 4096-bit case). The keys e and d satisfy $ed \equiv 1 \ \left(mod\ \varphi(n)\right)$, in other words, $d = e^{-1} \ \left(mod\ \varphi(n)\right)$. (Note: $\varphi(n) = (p-1)(q-1)$.)