MATH 3527 - Lecture Notes

Lucas Sta. Maria
stamaria.l@northeastern.edu

February 28, 2024

Contents

1 LECTURE 1

This is the first lecture.

2 LECTURE 4

January 17, 2024

Today: Properties of GCDs, proof of correctness for Euclid, primes

Definition 2.1

Two integers a, b are *relatively prime* if and only if $\gcd(a, b) = 1$.

Example 2.2

5 and 6 are relatively prime, since $gcd(5, 6) = 1$. However, 4 and 6 are not, since $gcd(4, 6) = 2 \neq 1$.

Theorem 2.3: Properties of GCDs.

Let a, b, c, d, m be integers.

1. If $m > 0$ then $\gcd(ma, mb) = m \gcd(a, b)$.

   Proof. $gcd(ma, mb)$ is the smallest positive integer of the form $x(ma) + y(mb)$. Since both are divisible by m, it is equivalent to the smallest positive integer of the form $m(xa + yb)$. That is further equivalent to m times the smallest positive integer of the form $xa + yb$. And so, it is equivalent to $m \cdot \gcd(a, b)$. $\square$

2. If $d > 0$ is a common divisor of a, b, then $\gcd(\frac{a}{b}, \frac{b}{d}) = \frac{\gcd(a,b)}{d}$.

   Proof. Consider $d \gcd(\frac{a}{b}, \frac{b}{d}) = \gcd(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}) = \gcd(a, b)$. $\square$

3. There exist integers x, y such that $xa + yb = 1$ if and only if $\gcd(a, b) = 1$.

   Proof. Suppose $\gcd(a, b) = 1$. We want to show there exist integers x, y such that $xa + yb = 1$. By the GCD property, there exist $xa + yb = \gcd(a, b) = 1$.

   Conversely, suppose there exist integers x, y with $xa + yb = 1$. 1 is certainly a common divisor. Now suppose d is some common divisor: Then, $d|a$ and $d|b$. So $d|(xa + yb)$, so $d = -1, 1$. So $d \leq 1$. $\square$

4. If a, b are relatively prime to m, so is $a \cdot b$.

   Proof. Since a, b are relatively prime to m, there exist integers x, y such that $xa + ym = 1$ and integers p, q such that $pb + qm = 1$. Multiplying,

   $$\begin{aligned} (xa + ym)(pb + qm) &= 1 \cdot 1 = 1 \\ xapb + xaqm + ympb + ymqm &= 1 \\ (xp)ab + (xaq + ypb + ymq)m &= 1 \end{aligned}$$

   So, ab, m are relatively prime. $\square$

5. For any integers a, b, x, $\gcd(a, b) = \gcd(a, b + xa)$.

   Proof. If $d|a$ and $d|b$, then $d|a$ and $d|(b + xa)$.

   If $e|a$ and $e|(b + xa)$, then $e|a$ and $e|((b + xa) - xa)$. $\square$

6. If $a|bc$ and a, b are relatively prime, then $a|c$. (*Relatively Prime Divisibility Property*, also known as *Fundamental Theorem of Arithmetic*)

   Proof. Since a, b are relatively prime, there exist integers x, y with $xa + yb = 1$. We know $a|bc$. We want to show $a|c$. Multiplying by c, $xac + ybc = c$. The terms on the LHS are divisible by a, since the first term xac contains a as a factor, and the second term ybc has b which is divisible by a. And, $xac + ybc$ is divisible by a since summing the terms together maintains their divisibility by a. $\square$

   Proof. Another proof. Observe that $\gcd(ac, bc) = c \cdot \gcd(a, b) = c$. Notice that $a|ac$ and $a|bc$. <u>Fact:</u> any common divisor of two numbers divides their gcd. So a divides $\gcd(ac, bc) = c$. $\square$

Definition 2.4

If $a|e$ and $b|e$, we say e is a common multiple of a, b. $lcm(a, b)$ is the smallest positive common multiple of a, b.

Example 2.5

$lcm(4, 5) = 20$ and $lcm(6, 8) = 24$.

Theorem 2.6: Properties of LCMs.

Let a, b, c, m be positive integers.

1. If $m > 0$ then $lcm(ma, mb) = m \cdot lcm(a, b)$.

   Proof. Observe $(ma)|lcm(ma, mb)$. In particular, $m|lcm(ma, mb)$ by transitivity. So, $lcm(ma, mb) = mk$. Note $ma|mk$, and also $mb|mk$. So, $a|k$ and $b|k$. So $k \geq lcm(a, b)$. But notice ma divides $m \cdot lcm(a, b)$. So, a divides $lcm(a, b)$. So, $m \cdot lcm(a, b)$ is a common multiple of ma, mb. So it's the smallest! $\square$

2. If a, b are relatively prime, then $lcm(a, b) = ab$.

   Proof. Obviously ab is a common multiple of a, b. So, now let l be a common multiple of a, b. Then, $a|l$ so $l = ak$ for some k. Also, $b|l$ so $b|ak$, and a, b are relatively prime. So, by (6) of GCDs, we see $b|k$. So, $k \geq b$, and so $l = ak \geq ab$. So, $lcm = ab$. $\square$

3. For any a, b we have $lcm(a, b) \cdot gcd(a, b) = ab$.

   Proof. Let $d = \gcd(a, b)$. Observe that $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{\gcd(a,b)}{d} = \frac{d}{d} = 1$. Then by (2), $lcm(\frac{a}{b}, \frac{b}{d}) = \frac{a}{d} \cdot \frac{b}{d}$. Then, $lcm(a, b) = d \cdot lcm(\frac{a}{d}, \frac{b}{d}) = d \cdot \frac{a}{d} \cdot \frac{b}{d} = ab$. $\square$

Definition 2.7: Euclidian Algorithm.

$$
\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1} \\
r_k &= q_{k+2} r_{k+1}
\end{aligned}
$$

Theorem 2.8

The Euclidian Algorithm always terminates and $gcd(a, b) =$ the last nonzero remainder.

Proof. The algorithm terminates because the remainders are strictly decreasing: $r_1 > r_2 > r_3 > \cdots \geq 0$. By the well-ordering axiom, this can't continue forever. $\square$

Theorem 2.9

For all $n \geq -1$, we have $\gcd(a, b) = \gcd(r_n, r_{n+1})$.

Proof. Induct on n.
Base case: $n = -1$. $\gcd(a, b) = \gcd(r_1, r_0) = \gcd(a, b)$ which is true by definition.
Inductive step: Suppose $\gcd(r_n, r_{n+1}) = \gcd(a, b)$. Consider $n + 1$. So, $r_{n+2} = r_n - q_{n+2}r_{n+1}$. So,

$$\begin{aligned}
\gcd(r_{n+1}, r_{n+2}) &= \gcd(r_{n+1}, r_n - q_{n+2}r_{n+1}) \\
&= \gcd(r_{n+1}, r_n) \\
&= \gcd(a, b)
\end{aligned}$$

By induction, $\gcd(a, b) = \gcd(r_{k+1}, 0) = k + 1$. □

Theorem 2.10

Each remainder r_n can be written as $r_n = x_n a + y_n b$.

Proof. Induct on n.
Base cases: $n = -1$: $r_{-1} = a = 1a + 0b$. $n = 0$: $r_0 = b = 0a + 1b$.
Inductive step: Suppose $r_{n-1} = x_{n-1}a + y_{n-1}b$ and $r_n = x_n a + y_n b$. Consider $n + 1$. Then,

$$\begin{aligned}
r_{n+1} &= r_{n+1} - q_{n+1}r_n \\
&= (x_{n-1}a + y_{n-1}b) - q_{n+1}(x_n a + y_n b) \\
&= (x_{n-1} - q_{n+1}x_n)a + (y_{n-1} - q_{n+1}y_n)b \\
&= x_{n+1}a + y_{n+1}b
\end{aligned}$$

as claimed. □

Definition 2.11

We say $p \in \mathbb{Z}_+$ it is *prime* if there is no integer d with $1 < d < p$ such that $d|p$. If $n \in \mathbb{Z}_+$ is not prime, we say it is *composite*.

3 LECTURE 5

January 18, 2024

Primes, Prime Factorization, Applications of Factorization

Definition 3.1

A *prime factorization* is a product of primes.

Theorem 3.2

Every positive integer n can be written as a product of primes.

Proof. Induct on n.
Base case: For $n = 1$, 1 is equivalent to the empty product of primes.
Inductive step: Suppose that all positive integers less than n have a prime factorization. If n is prime, then $n = n$. Otherwise, if n is composite, then $n = ab$ with $1 < a, b < n$. By the inductive hypothesis, both a, b ahev prime factorizations. Multiply them together to get a prime factorization for n. $\square$

Theorem 3.3: Prime Divisibility Property.

Suppose p is prime, and $p|ab$ for $a, b \in \mathbb{Z}$. Then, $p|a$ or $p|b$.

Proof. Consider $\gcd(a, p)$. Since p is prime, there are 2 options: 1 and p. If $\gcd(a, p) = p$, then $p|a$. Otherwise, if $\gcd(a, p) = 1$, then a and p are relatively prime. Since $p|ab$ and p is relatively prime to a, then by the relatively-prime divisibility property, $p|b$. $\square$

Theorem 3.4: Fundamental Theorem of Arithmetic.

Every positive integer n has a *unique* prime factorization up to reordering the factors.

Proof. Induct on n.
Base case: Consider $n = 1$. 1's prime factorization is the empty product: $1 = 1$. Any nonempty factorization has at least one prime.
Inductive step: Suppose every positive integer less than n has a unique prime factorization. Suppose $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ for primes p_i, q_i. Observe that p_1 divides $q_1 q_2 \cdots q_l$. By the prime divisibility property, p_1 divides one of the q_i. Rearrange the q_i such that p_1 divides q_1. The only possible divisor of q_1 is q_1. So, $p_1 = q_1$. $\square$

Proposition 3.5

Suppose $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$.

1. $a|b$ if and only if $a_i \leq b_i$ for all i.
2. $\gcd(a, b) = \prod_{i=1}^{k} p_i^{min(a_i, b_i)}$.
3. $lcm(a, b) = \prod_{i=1}^{k} p_i^{max(a_i, b_i)}$.

Proposition 3.6

Suppose $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ is some prime factorization.

1. The number of positive divisors of n equals $\prod_{i=1}^{k} (n_i + 1)$.
2. The sum of positive divisors of n equals $\prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{n_i})$.

4 LECTURE 7

January 24, 2024

Modular congruences, residue classes

Definition 4.1: ***Modular congruences.***

If m is a positive integer (the *modulus*), $a \cong b(\mod m)$ when $m|(b-a)$.

Example 4.2

- $1 \cong 11(\mod 5)$ since 5 divides $11 - 1 = 10$.
- $0 \cong 18(\mod 3)$ since 3 divides $18 - 0 = 18$.
- $2 \ncong 11(\mod 4)$ since 4 does not divide $11 - 2 = 9$

Proposition 4.3

Properties of modular congruences.

1. $a \cong a \mod m$

   Proof. $a \cong a \mod m$ says by definition that $m|(a-a)$ which is true, since $m|0$ $(0 = 0 \cdot m)$. □

2. If $a \cong b \mod m$ then $b \cong a \mod m$

   Proof. Suppose $a \cong b \mod m$. Then, $m|(b-a)$. So, $m|-(b-a)$ and $m|(a-b)$. So $b \cong a \mod m$. □

3. If $a \cong b \mod m$ and $b \cong c \mod m$ then $a \cong c \mod m$

   Proof. Suppose $a \cong b \mod m$ and $b \cong c \mod m$. Then, $m|(b-a)$ and $m|(c-b)$. So then $m|((c-b)+(b-a))$ and $m|(c-a)$. So, $a \cong c \mod m$. □

4. If $a \cong b \mod m$ and $c \cong d \mod m$, then $a + c \cong b + d \mod m$ and $ac \cong bd \mod m$.

   Proof. Suppose $a \cong b \mod m$ and $c \cong d \mod m$. Then $m|(b-a)$ and $m|(d-c)$. Adding, $m|((b-a)+(d-c))$ so $m|((b+d)-(a+c))$. So, $a+c \cong b+d \mod m$.

   For multiplication: $m|(b-a)$ implies that there exists some k such that $b - a = km$ and $m|d-c$ implies that there exists some l such that $d-c = lm$. So, $b = a+km$ and $d = c+lm$. Then, $bd-ac = (a+km)(c+lm)-ac = ac+kmc+alm+kmlm-ac$. This simplifies to $m(kc+al+kml)$. And kml is some integer, so $m|(bd-ac)$.

   Alternative proof for multiplication. Since $m|(b-a)$ and $m|(d-c)$, m also divides $d(b-a)+a(d-c)$. This expands to $bd-ad-ad-ac = bd-ac$. □

Remark 4.4

Congruence behaves a lot like equality. The first three properties of congruences is an *equivalence relation.*

Remark 4.5

Philosophy: congruence is a somewhat weaker version of equality. Saying that $a \cong b \mod m$ says that a equals b up to adding/subtracting a multiple of m.

Definition 4.6

If m is a modulus, and a is any integer, the *residue class* of $a \mod m$ is the set

$$\bar{a} = \{b \in \mathbb{Z} : a \cong b \mod m\}$$

of all integers b congruent to $a \mod m$. Also could be

$$\{a + km : k \in \mathbb{Z}\}$$

Example 4.7

Consider $m = 5$.

$$\begin{aligned}\bar{6} &= \{\ldots, -9, -4, 1, 6, 11, 16, 21, \ldots\}\\ \bar{1}1 &= \{\ldots, -9, -4, 1, 6, 11, 16, 21, \ldots\}\end{aligned}$$

Proposition 4.8

Properties of residue classes. Let m be a modulus and $a, b \in \mathbb{Z}$.

1. $\bar{a} = \bar{b}$ if and only if $a \cong b \mod m$.

   Proof. Suppose $\bar{a} = \bar{b}$. Observe that $b \in \bar{b}$ since $b \cong b \mod m$. But since $\bar{a} = \bar{b}$, that means $b \in \bar{a}$. So $a \cong b \mod m$.

   Conversely, suppose $a \cong b \mod m$. WLOG for a and b, we want to show $\bar{a} \subseteq \bar{b}$. Let $c \in \bar{a}$. Since $c \in \bar{a}$, that means $a \cong c \mod m$. We also know $a \cong b \mod m$. So by the symmetry property, $b \cong a \mod m$. Then $b \cong a \mod m$ and $a \cong c \mod m$. So $b \cong c \mod m$ by transitivity. □

2. Two residue classes are either disjoin or identical.

   Proof. Suppose $\bar{a}, \bar{b}$ are residue classes. If they have no elements in common, we are done. Otherwise, they have some element in common, c. Then, $c \in \bar{a}$ and $c \in \bar{b}$. Then by definition, $a \cong c \mod m$ and $b \cong c \mod m$. Then $a \cong c \mod m$ and $c \cong b \mod m$ and so $a \cong b \mod m$ by transitiivity. So, $\bar{a} = \bar{b}$. □

3. There are exactly m distinct residue classes.

   Proof. Suppose a is an integer. Divide a by m: $a = qm + r$ where $0 \leq r < m$. Observe that $r - a = -qm$. So, $m|(r - a)$, $a \cong r \mod a$, and $\bar{a} = \bar{r}$. So any residue class equals one of $\bar{0}, \bar{1}, \ldots, m \bar{-} 1$. □

Example 4.9

Residue class arithmetic. $m = 5$. These are equivalent:

- $\bar{1} + \bar{1} = \bar{2}$
- $\overline{11} + \bar{6} = \overline{17}$

5 LECTURE 12

February 5, 2024

Properties of Orders, The Euler ϕ-Function

Last time: *Fermat's Little Theorem, Wilson's Theorem, Orders*

Definition 5.1

If u is a unit modulo m, the smallest $k > 0$ such that $u^k \cong 1 \mod m$ is called the *order* of u.

Proposition 5.2

Properties of orders.

1. If $a^n \cong \mod m$, then the order of a divides n.

   Proof. Let k be the order of a. Suppose $a^k \cong 1 \mod m$. Divide n by k: $n = qk + r$ for $0 \leq r \leq k$. Observe

   $$\begin{aligned} 1 \cong a^n &= a^{qk+r} \\ &= (a^k)^q a^r \mod m \\ &= 1^q \cdot a^r \mod m \\ &= a^r \mod m \end{aligned}$$

   So $a^r \cong 1 \mod m$, r can't be positive as that would contradict definition of the order being k. So, $r = 0$, and thus $k|n$. □

2. If a has order k, then a^w has order $k/\gcd(w,k)$.

   Proof. Suppose $(a^w)^b \cong 1 \mod m$, then $a^{wm} \cong 1 \mod m$. So, by (1), the order of a (k) divides $w \cdot b$. Divide through $\gcd(w,k)$: $\frac{k}{\gcd(w,k)}$ divides $\frac{w}{\gcd(w,k)} b$ but $\frac{k}{gcd}$ is relatively prime to $\frac{w}{gcd}$. So by relative prime divisibility theorem, $\frac{k}{\gcd(w,k)}$ divides b. So $a^w \cong a^k$. □

3. $\bar{a}$ has order n if and only if $a^n \cong 1 \mod m$ and $a^{k/p} \ncong 1 \mod m$ for any prime divisor p.

Definition 5.3

If m is a modulus, the *Euler ϕ-function* $\phi(m)$ is the number of units in $\mathbb{Z}/m\mathbb{Z}$. Equivalently, $\phi(m)$ is the number of integers between 1 and m inclusive that are relatively prime to m.

Proposition 5.4

Properties of $\phi(m)$.

1. If p is prime then $\phi(p^k) = p^k - p^{k-1}$.
2. For any relatievly prime a, b we have $\phi(ab) = \phi(a) \cdot \phi(b)$.
3. If m has prime factorization $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ then $\phi(m) = \phi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ which results in $(p_1^{m_1} - p_1^{m_1 - 1}) \cdots$

6 LECTURE 14

February 8, 2024

Repeating Decimals, Introduction to Cryptography

Last time: *Euler's Theroem, Primitive Roots*

Next Time: *Rabin + RSA Encryption*

Remark 6.1

We identify three separate behaviours for decimals:

1. Terminating decimal ($\frac{1}{2}, \frac{1}{4}, \ldots$)
2. Immediately periodic ($\frac{1}{3}, \frac{1}{7}, \ldots$)
3. Eventually periodic ($\frac{1}{6}, \frac{1}{12}, \ldots$)

What is the pattern? How do we determine which category a fraction will belong in? Consider a decimal

$$\begin{aligned} &\frac{d_1}{10} + \frac{d_2}{100} + \frac{d_3}{1000} + \cdots + \frac{d_k}{10^k} \\ &= \frac{d_1 d_2 d_3 \cdots d_k}{10^k} \end{aligned}$$

So, for the terminating decimal cases, the denominator divides a power of 10.
What is the value of $0.d_1 d_2 \cdots d_k$ as a rational number $\frac{p}{q}$? Consider

$$\begin{aligned} 0.\bar{1}\bar{4} &= 0.141414\ldots \\ &= \frac{1}{10^1} + \frac{4}{10^2} + \frac{1}{10^3} + \cdots \\ &= (\frac{1}{10} + \frac{1}{10^3} + \cdots) + (\frac{4}{10^2} + \frac{4}{10^4} + \cdots) \end{aligned}$$

We *could* do a geometric series, but that's quite annoying. Instead, let's do this.
$100x = 14.141414\ldots$ and $x = 0.141414\ldots$, so $100x - x = 99x = 14.141414\ldots - 0.141414\ldots$ and so $99x = 14$ and thus $x = \frac{14}{99}$.
Generalizing this, for $x = 0d_1d_2d_3 \cdots d_k$, $10^k x = d_1 d_2 \ldots d_k.d_1 d_2 \bar{\cdots} d_k$, and so $10^k x - x = (10^k - 1)x = d_1 d_2 \cdots d_k$. So $x = \frac{d_1 d_2 \cdots d_k}{10^k - 1}$.

Proposition 6.2

When q is relatively prime to 10 and $\frac{p}{q}$ is in lowest terms, then the period of the repeating decimal is the order of $10 \mod q$. If k is the order, then $\frac{p}{q} = 0.d_1 d_2 \ldots d_k$ with $d_1 d_2 \ldots d_k = (10^k - 1) \cdot \frac{p}{q}$.

Cryptography

"Cryptos" in Greek means *hidden*, and "graphy" means *writing*. *Hidden writing*. *Cryptography* is the study of how to transmit information securely.

7 LECTURE 15

February 12, 2024

Rabin Encryption

Last time: *Repeating Decimals, Introduction to Cryptography*

Next Time: *RSA Encryption*

General Setup: Alice has a message (her *plaintext*) that she wants to send to Bob. She encrypts her message to obtain her *ciphertext* which she then sends to Bob. Bob receives the ciphertext and then decodes it to recover Alice's plaintext.

Definition 7.1

In a *Caesar Shift*, we shift all letters in plaintext forward a fixed number of letters to encrypt, and shift back to decrypt.

Remark 7.2

Caesar Shift is not very good:

- There are a fixed number of possible encryptions
- Both parties need to know the key
- Very easy to brute-force all possible decryptions

Definition 7.3

In *symmetric encryption*, the information needed to encode is equivalent to the information needed to decode.

Remark 7.4

Imagine Eve is eavesdropping and she overhears that the first word in the message is "Hi". With a Caesar Shift, she can easily figure out the key just from the small part of ciphertext, immediately figuring out the entire decryption. This is known as a *plaintext attack.*

Remark 7.5

We can improve the Caesar Shift by shifting letters by different amounts. However, this is subject to *frequency analysis* since some letters are more common than others.

Remark 7.6

We have several very secure symmetric cryptosystems: AES. With 128-bit AES and 32 rounds it'll take an unreasonable amount of time to brute-force something.

Definition 7.7

Asymmetric encryption (*public-key cryptosystems*) is secure enough that you can post the encryption method publically, but nobody can feasibly decrypt it except for you.

Remark 7.8

How does this work? We need a "one-way function": a function that's easy to evaluate but hard to invert.

Example 7.9

Consider $f(p, q) = pq$. It is not challenging to evaluate (although not pleasant).

Proposition 7.10

If $p \cong 3 \mod 4$ is a prime, and c is a square modulo p, then the solutions to $x^2 \cong c \mod p$ are $x \cong \pm c^{(p+1)/4} \mod p$.

Proof. Suppose $c \cong m^2 \mod p$. Then the solutions of $x^2 \cong c \cong m^2 \mod p$ are $(x+m)(x-m) \cong 0 \mod p$. So, $p|(x-m)(x+m)$ so $p|(x-m)$ or $p|(x+m)$ so $x \cong m \mod p$ or $x \cong -m \mod p$. These are two solutions which are negatives of each other.
We have

$$\begin{aligned} x^2 &\cong (c^{(p+1)/4})^2 \mod p \\ &\cong (m^2)^{(p+1)/2} \mod p \\ &\cong m^{p+1} \mod p \\ &\cong m^{p-1} \cdot m^2 \mod p \\ &\cong 1 \cdot c \cong c \mod p \end{aligned}$$

So $x^2 \cong c \mod p$. □

Definition 7.11

Rabin Encryption.

1. Alice converts her message to a residue class m modulo n. She computes $m^2 \mod n = c$ and sends it to Bob.
2. Bob has to solve the equation $x^2 \cong c \mod n$. Using $n = pq$, Bob solves $x^2 \cong c \mod pq$ and he knows that both $x^2 \cong c \mod p$ and $x^2 \cong c \mod q$. By the above claim, we can use the Chinese Remainder Theorem to solve $x \cong \pm c^{(p+1)/4} \mod p$ and $x \cong c^{(q+1)/4} \mod q$ to get solutions modulo $n = pq$.

Remark 7.12

How secure is Rabin Encryption? If Eve is eavesdropping, she has the following information: the value n and the ciphertext c. She only knows the product of the two primes – she has to solve the equation $x^2 \cong c \mod m$. However, factorization is hard. Is there another way to find p and q without factoring n? No!

Remark 7.13

If $n = pq$ is the product of two distinct primes, and c is any cipher mod n, finding the four solutions to $x^2 \cong c \mod n$ is equivalent to factoring n.

Remark 7.14

Now suppose Eve has the four square roots of $c \mod n$. The solutions are $\pm m \mod n$ and $\pm w \mod n$. Consider $m + w \cong m + (-m) \cong 0 \mod p$ and $m + w \cong m + m \cong 2m \mod q$. By Euclid, $\gcd(m + w, pq) = p$. Factor!

Remark 7.15

Breaking Rabin encryption for a single message (finding all 4 decodings) is equivalent to factoring the modulus. This means you don't want to use Rabin encryption practically since it's vulnerable to a very serious kind of attack.
Suppose Eve sneaks in and uses Bob's decryption computer. She steals the factorization. She takes a random m and asks the computer to decode m^2. Computer will return one of the four possible encodings: $m, -m, w, -w$. If she gets $m, -m$ she tries again. If she gets $w, -w$, she uses Euclid's algorithm and find's the factorization. Every time she does this, she has a 50% change of factoring n.

8 LECTURE 16

February 14, 2024

RSA Encryption

Last time: *Rabin Encryption*

Next time: *Zero-Knowledge Proofs*

What are the issues with Rabin? Since the encoding function is not one-to-one, there is a nonuniqueness of square roots.

What if we did encryption as $c = m^e \mod n$ (for some $e \neq 2$)? What conditions on e are needed so that every encrypted message c has a unique decoding?

For some e, we want the only solution to $x^e \cong 1 \mod n$ to be $x = 1$. We want to have no elements of order dividing e, except $x = 1$.

Since we want orders of units modulo n dividing $\phi(n)$, we need e and $\phi(n)$ to be relatively prime. And so the encryption function $f(x) = x^e \mod n$ is invertible – each encrypted message has a unique decoding.

Definition 8.1: RSA Encryption

1. Bob sets up his public key n, e. n is the product of two primes p, q. e is any integer greater than 1 relatively prime to $\phi(n) = (p-1)(q-1)$. Bob publishes n, e but keeps p, q secret.
2. Alice wants to send Bob a message m. She encrypts by computing $c \cong m^e \mod n$.
3. Bob receives a ciphertext c and needs to decrypt it. Bob computes $c^d \mod n$ where d is the multiplicative inverse of $e \mod \phi(n)$.

Remark 8.2

Since e is relatively prime to $\phi(n)$, e is a unit modulo $\phi(n)$. So it has a multiplicative inverse d, with $de \cong 1 \mod \phi(n)$. So $de = 1 + k\phi(n)$ for some integer k.

$$\begin{aligned} c^d &\cong m^{de} \mod n \\ &\cong m^{1+k\phi(n)} \mod n \\ &\cong m^1 \cdot m^{k\phi(n)} \mod n \\ &\cong m \cdot (m^{\phi(n)})^k \mod n \\ &\cong m \cdot 1^k \mod n \\ &\cong m \end{aligned}$$

Remark 8.3

Why is RSA secure?
Eve knows n, e since they are public. She also has the encrypted message c. So, she must find m by solving $x^e \cong c \mod n$.

1. She could solve for n, then decrypt it just as Bob does. This is infeasible in terms of time.
2. Can eve just find some decryption exponent d? $\frac{d \cdot e - 1}{n} \approx \frac{d \cdot e - 1}{\phi(n)}$. Eve now has n and $\phi(n)$ and compute the prime factorization of n. Still difficult.

Remark 8.4

With RSA, there are two things Eve might want.

1. Decrypt a single message
2. Decrypt all possible messages
   Message-padding solves these problems.

9 LECTURE 17

February 15, 2024

Zero-Knowledge Proofs

Last time: *RSA Encryption*

Remark 9.1

In Rabin/RSA, participants have no way of authenticating each other's identities. What we want is a way to authenticate identity.

Remark 9.2

Peggy the prover wants to establish her identity to Victor the verifier. Peggy has a secret that she cannot share, otherwise somebody else could impersonate Peggy. She needs to prove to Victor that she knows the secret without revealing the secret information.
The idea of a *zero-knowledge* proof is to prove something without revealing it.

Remark 9.3

Conversation.
Peggy: I can count the number of leaves on any tree instantaneously.
Victor: I'm skeptical.
Peggy: Okay, that tree has $41,815$ leaves.
Victor: Okay, how am I going to check that?

Remark 9.4

Protocol:

1. Peggy counts the number of leaves on the tree. She looks away.
2. Victor either removes a leaf or doesn't.
3. Peggy looks at the tree again, and tells Victor if a leaf was taken off.
4. Repeat multiple times, so it's not up to chance.

The probability of her lying would be incredibly low.

Remark 9.5

Victor should be convinced. Should Eve be convinced? No! Peggy and Victor could be conspiring to make it seem like Peggy passes.

Definition 9.6

Rabin Zero-knowledge Protocol

1. Peggy finds two large primes p, q and computes $N = pq$. She also picks her secret number s, some residue class modulo N. She publishes $N, s^2 \mod N$ and keeps p, q, s secret. Peggy wants to prove she knows s.

2. Victor challenges Peggy to verify her identity.

   (a) Peggy picks a random unit $u \mod N$. She computes $u^2 \mod N$ and sends it to Victor.

   (b) Victor then asks either for u or $su \mod n$. Peggy sends what he requests.

   (c) Victor verifies her sent value. If he asked for u, he knows N, squares $(u)^2$ to u^2 from earlier. Otherwise, if he asked for su, he compares the square $(su)^2$ to s^2u^2, since s^2 is public and u^2 was received.

3. Challenge done.

Remark 9.7

3 components to zero-knowledge protocol:

1. *Complete*: Peggy can always pass

2. *Sound*: Eve can't always pass

3. *Zero-knowledge*: Even doesn't learn anything about s by observing Peggy and Victor

   (a) u^2

   (b) For u, Eve knows nothing about u. For su, Eve needs to be able to find u, which requires computing square root modulo N.

Remark 9.8

Authentication protocol:

1. Alice and Bob set up RSA keys.

2. They send each other messages.

3. They use the zero-knowledge protocol to establish that each message was received and decoded.

10 LECTURE 18

February 26, 2024

Primality and Compositeness Testing

Next time: *Factoring Algorithms*

Given a large integer m, how can we reasonably and quickly decide whether m is prime?

- If m is prime, how can we prove it?
- If m is composite, how can we factor it?

Consider the contrapositive of Format's Little Theorem: if $a^m \ncong a \mod m$ for some a, then m is composite.

Definition 10.1: Fermat Test

If $a^m \ncong a \mod m$ for some a, then m is composite. Test some integer several times with the statement.

Example 10.2

Test the compositeness of $m = 56011607$.
Trivially, $a = \bar{0}$ and $a = \bar{1}$ are not useful. So, we should consider $a = 2$. With Mathematica, we have determined this to be composite, since it satisfies the contrapositive of Fermat's Little Theorem.

Example 10.3

Test the compositeness of $m = 341$.
For $a = 2$, $2^{341} \cong 2 \mod 341$. Since the hypothesis doesn't hold, this is inconclusive! We must try another value.
For $a = 3$, $3^{341} \cong 168 \mod 341$. So, m is composite.

Example 10.4

Test the compositeness of $m = 561 = 3 \cdot 11 \cdot 17$.
For $a = 2$, $2^{561} \cong 2 \mod 561$: inconclusive.
For $a = 3$, $3^{561} \cong 3 \mod 561$: inconclusive.
For $a = 5$, $3^{561} \cong 5 \mod 561$: inconclusive.
For $a = 7$, $3^{561} \cong 7 \mod 561$: inconclusive.
In fact, $a^{561} \cong a \mod 561$ for every integer a. Why? We know $561 = 3 \cdot 11 \cdot 17$. So, it's enough to show that $a^{561} \cong a \mod 3, 11, 17$. By Fermat's Little Theorem, $a^{561} \cong a^{21} \cong a^{11} \cong a \mod 11$. Same with modulo 3 and modulo 17.

Note that it is enough to check just the primes for the composite test.

Definition 10.5: Carmichael Number

An composite integer m such that $a^m \cong a \mod m$ for all a is a *Carmichael number.*

There are infinitely many Carmichael numbers, but they are significantly less common than primes.

Recall that if p is prime, then the only solutions to $x^2 \cong 1 \mod p$ are $x \cong \pm 1 \mod p$. The contrapositive is: if $x^2 \cong 1 \mod m$ and $x \ncong \pm 1 \mod m$, then m is composite. However, if $m = pq$ then there are four solutions to $x^2 \cong 1 \mod pq$.

Example 10.6

For $m = 341$, $a = 2$, we find $2^{341} \cong 1 \mod 341$.
Look at $2^{170} \cong 1 \mod 341$. Now try $2^{85} \cong 32 \mod 341$. Since $32^2 \cong 1 \mod 341$ and $32 \ncong 1 \mod 341$, then 341 is composite!

Definition 10.7: Miller-Rabin Test

Suppose m is an integer, and $m - 1 = 2^d k$ where k is odd. Compute the list $\left\{a^k, a^{2k}, a^{4k}, \dots, a^{2^d k}\right\} \mod m$.

- If the last entry a^{m-1} is not congruent to $1 \mod m$, then m is composite.
- If the last entry a^{m-1} is congruent to $1 \mod m$, and there is a 1 on the list preceded by an entry not ± 1, m is composite.
- Otherwise, test is inconclusive.

Are there any integers for which Miller-Rabin always fails? No! If m is composite, then at least $\frac{3}{4}$ of the residue classes $a \mod m$ will show m is composite with Miller-Rabin.

For the "primality test", we can test 100 random $a \mod m$ with Miller-Rabin. The probability of having an inconclusive test all 100 times is less than $(\frac{1}{4})^{100}$.

If you assume the Generalized Riemann Hypothesis, then it's known that Miller-Rabin succeeds after testing the first $2 \log m$ values of a. With the assumption, this gives a polynomial-time algorithm.

Do we have a provable primality test that runs "fast"? Yes, the AKS test. With the AKS test, we can do provable primality testing in about $(logm)^{12}$ time. Generally slow.

Definition 10.8: AKS Test

m is a prime if and only if $(x + a)^m \cong x^m + a \mod m$ for any $a \mod m$.

AKS is clearly too much calculation to do. Instead, compute $(x + a)^m - x^m - a \mod (x^r - 1, m)$ for various small r. Together with the Chinese Remainder Theorem, we get $(x + a)^m \cong x^m + a \mod m$.

How can we prove a given p is prime? p is prime if and only if there is a unit $a \mod p$ of order $p - 1 = \phi(p)$. If p is prime, take a to be a primitive root. There's only $p - 1$ possible units modulo p (everything other than 0). So, if a has order $p - 1$, then there are $p - 1$ units modulo p: $\{1, 2, \dots, p - 1\} \mod p$. This gives a way to show p is prime.

Definition 10.9: Lucas Primality Criterion

If there exists $a \mod m$ with $a^{m-1} \cong 1 \mod m$ and $a^{(m-1)/p} \ncong 1 \mod m$ for any p dividing $m - 1$, then m is prime.

Remark 10.10

There are 2 challenging things regarding the Lucas Primality Criterion.

- Need a factorization of $m - 1$ – factoring is hard.
- Need to find a primitive root modulo m – you would need to test everything.

Example 10.11

Show 2029 is prime. Then, $2028 = 2^2 \cdot 3 \cdot 13^2$. Now, test $a = 2$. So, $2^{2028} \cong 1 \mod 2029$. And $2^{2028/2} \cong -1 \mod 2029$. And $2^{2028/3} \cong 975 \mod 2029$ and finally $2^{2028/13} \cong 302 \mod 2029$. So, the order of 2 is 2028. Thus, 2029 is prime!

11 LECTURE 19

February 28, 2024

Factorization Algorithms

Next time: $\mathbb{Z}(\sqrt{0})$, $F[x]$, *and Euclidean Domains*

Definition 11.1: Fermat Factorization

If $n = pq$, and p, q are odd, then $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ – the difference of squares. Conversely, if $n = a^2 - b^2 = (a-b)(a+b)$, then the factorization has $a > b + 1$. To search for a, b with $n = a^2 - b^2$, estimate $\sqrt{n}$, round up, and test those values for a.

Example 11.2

Factor $n = 1298639$.
We estimate $\sqrt{n} \approx 1139.58$. Try $a = 1140$: $1140^2 - n = 961 = 31^2$. So, $n = 1140^2 - 31^2 = (1140 - 31)(1140 + 31) = 1109 \cdot 1171$.

Example 11.3

Factor $n = 2789959$.
We estimate $\sqrt{n} = 2282$. Try $1161^2 - n = 2282$, not square. Try $1672^2 - n = 5625 = 75^2$. $n = (1675 - 75)(1675 + 75) = 1597 \cdot 1747$.

Example 11.4

Fermat Factorization is quick when the factors p, q of $n = pq$ are close together.

Idea: Let $n = pq$. If we pick a random unit $a \mod n$. Its order modulo p probably is different from its order modulo p. If k is the order of $a \mod p$, then $a^k \cong 1 \mod p$ but $a^k \ncong 1 \mod q$. So $a^k - 1$ is divisible by p but not q. What is $\gcd(a^k - 1, pq) = p$. Since the Euclidean algorithm is very fast, we can use it. So k is a multiple of the order of $a \mod p$ and isn't a multiple of the order of $a \mod q$. So, try a bunch of k and hope we find one divisible by the order $a \mod p$ but not the order $a \mod q$.

Definition 11.5: Pollard's $p - 1$-Factorization Algorithm

Let n be composite. Choose any $a > 1 \mod n$ and a bound b.

1. Set $x_1 = a$. For each $2 \le j \le b$, set $x_j = x_{j-1}^j \mod n$ and compute $\gcd(x_j - 1, n)$ at each step.
2. When $1 < \gcd < n$, get the factor.
3. When $\gcd = 1$, need to increase b.
4. If $\gcd = n$, pick a different a.