Tuesday’s lecture:
- One-way permutations (OWPs)
- PRGs from OWPs

Today’s lecture:
- Basic number theory

So far: "secret key" cryptography

Going forward: "public key" cryptography
Divisibility

- The set of integers is $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Let $a$ and $b$ be any two integers

**Def**: $b$ is called a divisor of $a$ if $\exists c \in \mathbb{Z}$ such that $a = bc$

We write $b \mid a$ (read “$b$ divides $a$”) to indicate that $b$ is a divisor of $a$ and $b \nmid a$ to indicate that $b$ is not a divisor of $a$

- If $b \mid a$, then $a$ is called a multiple of $b$

**Def**: $a$ is called a prime if $a > 1$ and $b \mid a$ implies that $b \in \{\pm 1, \pm a\}$
Divisibility

- Does 6 divide 12?  YES!  (Because $6 \cdot 2 = 12$)
- Does 6 divide 6?  YES!  (Because $6 \cdot 1 = 6$)
- Does 0 divide 6?  No!  (Because $0 \cdot c = 0$ for all $c \in \mathbb{Z}$)
- Does 6 divide 0?  YES!  (Because $6 \cdot 0 = 0$)
- Does 4 divide 6?  No!  (Because $4 \cdot 1 < 6$ and $4 \cdot 2 > 6$)
- Does 1 divide 6?  Yes!  (Because $1 \cdot 6 = 6$)
**Division Algorithm**

**Thm:** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$ and $0 \leq r < b$.

The integer $q$ is called the **quotient** and $r$ the **remainder** upon division of $a$ by $b$.

- If $b \mid a$, then $r = 0$.
- If $b > a$, then $q \geq 0$ and $r \geq 0$.
  
  - $a = 17$ and $b = 5$ $\Rightarrow$ $q = 3$ and $r = 2$, since $17 = 5 \cdot 3 + 2$
  - $a = -23$ and $b = 6$ $\Rightarrow$ $q = -4$ and $r = 1$, since $-23 = 6 \cdot (-4) + 1$
  - $a = 20$ and $b = 5$ $\Rightarrow$ $q = 4$ and $r = 0$, since $20 = 5 \cdot 4 + 0$
Greatest common divisors (GCDs)

Def.: The greatest common divisor of two non-zero integers $a$ and $b$ is the largest positive divisor of $a$ that is also a divisor of $b$.

The greatest common divisor of $a$ and $b$ is denoted $\text{gcd}(a, b)$.

- $\text{gcd}(4, 15) = 1$?
- $\text{gcd}(4, 10) = 2$?
- $\text{gcd}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$

Def.: $a$ and $b$ are relatively prime if $\text{gcd}(a, b) = 1$
a.k.a co-prime

Ryan Henry
Least common multiples (LCMs)

**Defn:** The least common multiple of two non-zero integers \( a \) and \( b \) is the smallest positive multiple of \( a \) that is also a multiple of \( b \).

The least common multiple of \( a \) and \( b \) is denoted by \( \text{lcm}(a, b) \).

- \( \text{lcm}(4, 15) = 60 \quad (4 = 2^2 \text{ and } 15 = 3 \cdot 5) \)
- \( \text{lcm}(4, 10) = 20 \quad (4 = 2^2 \text{ and } 10 = 2 \cdot 5) \)
- \( \text{lcm}(4, 8) = 8? \quad (4 = 2^2 \text{ and } 8 = 2^3) \)
- \( \text{lcm}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2 \)
Properties of GCDs and LCMs

- Let \( a, b \in \mathbb{Z} \) with \( a > 0 \) and \( b > 0 \), let \( d = \gcd(a, b) \) and let \( m = \operatorname{lcm}(a, b) \). Then
  1. \( a \cdot b = d \cdot m \)
  2. If \( c \mid a \) and \( c \mid b \), then \( c \mid d \)
  3. If \( a \mid s \) and \( b \mid s \), then \( m \mid s \)

Bezout's identity: There exist integers (unique) \( s \) and \( t \) such that \( d = as + bt \)

"gcd is a linear combination"
Extended Euclidean Algorithm

Fact 1: If \( b \mid a \), then \( \gcd(a, b) = b \)

Fact 2: If \( a = b \cdot q + r \), then \( \gcd(a, b) = \gcd(b, r) \)

(Assume that \( a > b \); if not, swap \( a \) and \( b \))

Idea: Apply Facts 1 and 2 repeatedly, using the Division Algorithm to write \( a = b \cdot q + r \) at each step.

Pseudocode:

```python
function gcd(a, b) {
    while (a ≠ b) {
        if (a > b) {
            a := a − b;
        } else {
            b := b − a;
        }
    }
    return a;
}
```

\[
\begin{align*}
    a &= q_0 b + r_0 \\
    b &= q_1 r_0 + r_1 \\
    r_0 &= q_2 r_1 + r_2 \\
    r_1 &= q_3 r_2 + r_3 \\
    & \vdots \\
    r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\
    r_{k-2} &= q_{k-4} r_{k-3} + r_{k-4} \\
    & \vdots \\
    r_0 &= a - q_0 b \\
    r_1 &= b - q_3 r_0 \\
    & \vdots \\
    \gcd(a, b) &= r_{k-3} - q_{k-1} r_{k-2}
\end{align*}
\]
Euclid's Lemma

Euclid’s Lemma: Let $a$ and $b$ be integers. If $p$ is a prime such that $p | a \cdot b$, then $p | a$ or $p | b$ (or both).

Proof: Assume W.L.O.G. that $p$ is prime and $p | a \cdot b$ but $p \nmid a$. We prove that $p | b$.

First note that $p \nmid a$ with $p$ prime implies that $\gcd(a, p) = 1$; thus, by Bezout’s Theorem, there exist integers $s$ and $t$ such that $as + pt = 1$.

Multiplying both sides of this expression by $b$ yields $bas + bpt = (ab)s + p(bt) = b$. Now, $p | (ab)s$ by assumption and clearly $p | p(bt)$; hence, $p | (bas + bpt)$. But $bas + bpt = b$ and it therefore follows that $p | b$, as desired. □
Fundamental Theorem of Arithmetic

**Fundamental Theorem of Arithmetic:** Let \( n > 1 \) be an arbitrary integer. Then \( n \) is a product of (powers of) primes, and this product is unique (up to the order of the prime powers).

- In other words, every \( n > 1 \) can be "factored" into primes in one- and only one- way.
Clock arithmetic

Q: If it is 10:00 am now, what time will it be in 6 hours?
A: 4:00 pm

Q: If it is 2:00 pm now, what time was it 3 hours ago?
A: 11:00 am

Q: It is currently October. What month will it be 25 months from now?
A: November

Q: On Mercury, each day is 1407 hours long. If it is 12:0000 now, what time will it be in 500 hours?
A: 2:300 (\approx 17:0000 - 14:0700)
Modular arithmetic

**Defn:** Let $a$, $r$, $n \in \mathbb{Z}$ with $n > 1$ and $0 \leq r < n$. Then $a$ is congruent to $r$ modulo $n$ if $a = q \cdot n + r$, as in the Division Algorithm.

We write $a \equiv r \mod n$ to indicate that $a$ is congruent to $r$ modulo $n$.

- $3 \equiv 1 \mod 2$
- $6 \equiv 0 \mod 2$
- $11 \equiv 2 \mod 3$
- $62 \equiv 62 \mod 85$

**Thm:** Let $a$, $b$, and $n$ be integers with $n > 1$, then $a \equiv b \mod n$ if and only if $n \mid a - b$. 

Ryan Henry
Notational conventions

- $p$ and $q$, typically denote prime numbers.
- $n$ is always a positive integer, which may or may not (though usually not) be prime.
- $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ with arithmetic modulo $n$.
- $\mathbb{Z}_n^* := \{ a \in \mathbb{Z}_n \mid \gcd(a, n)=1 \}$ with arithmetic modulo $n$. 

\textit{Ryan Henry}
Modular inversion

**Defn:** Let $a \in \mathbb{Z}_n$. The (multiplicative) inverse of $a$ modulo $n$ is an element $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \mod n$.

The inverse of $a$ modulo $n$ is denoted by $a^{-1}$.

- $2^{-1} \equiv ? \mod 3$ (since $2 \cdot 2 = 4 = 3 \cdot 1 + 1 \equiv 1 \mod 3$)
- $3^{-1} \equiv ? \mod 5$ (since $3 \cdot 2 = 6 = 5 \cdot 1 + 1 \equiv 1 \mod 5$)
- $2^{-1} \equiv ? \mod 6$ (i.e., the inverse does not exist!)
- Let $n$ be any odd integer. Then $2^{-1} \equiv (n+1)/2 \mod n$.
Modular inverses

Q: Which elements of $\mathbb{Z}$ have inverses modulo $n$?

Thm: An integer $a \in \mathbb{Z}$ has an inverse modulo $n$ if and only if $\text{gcd}(a, n) = 1$.
- Thus, $a \in \mathbb{Z}_n$ has an inverse modulo $n$ if and only if $a \in \mathbb{Z}_n^*$

Corollary: If $p$ is a prime, then $a$ has an inverse modulo $p$ if and only if $a$ is not a multiple of $p$; i.e., $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

Q: Given $a \in \mathbb{Z}_n^*$, how do you compute $a^{-1} \mod n$?

A: By definition, $a \cdot a^{-1} \equiv 1 \mod n \Rightarrow a \cdot a^{-1} = 1 + t \cdot n$ for some $t$
Hence, $a \cdot a^{-1} + (-t) \cdot n = \text{gcd}(a, n) \Rightarrow a^{-1} \equiv s$ from Bezout's Theorem
Thus, we can use the Extended Euclidean Algorithm
Solving linear equations modulo \( n \)

**Thm:** For any integer \( n > 1 \), there exists an integer \( x \) such that \( ax \equiv b \pmod{n} \) if and only if \( \gcd(a, n) \mid b \).

Q: Does \( 6x \equiv 18 \pmod{36} \) have a solution?
A: YES! Because \( \gcd(6, 18) = 6 \) and \( 6 \mid 18 \)
    In fact, it has 6 solutions in \( \mathbb{Z}_n \): 3, 9, 15, 21, 27, 33

Q: Does \( 2x \equiv 5 \pmod{10} \) have a solution?
A: NO! Because \( \gcd(2, 10) = 2 \) and \( 2 \nmid 5 \)
**Fermat's Little Theorem**

Fermat's Little Theorem: Let $p$ be a prime. Then for every $a \in \mathbb{Z}_p^*$, we have $a^{p-1} \equiv 1 \mod p$.

- **Corollary**: For all $a \in \mathbb{Z}_p$, $a^p \equiv a \mod p$.
  - $3^4 \equiv 1 \mod 5$
  - $84^{112} \equiv 1 \mod 113$
  - $79^{561} \equiv 79 \mod 113$ (since $561 = 5 \cdot (113 - 1) + 1$)

- **Trick**: To compute $a^x \mod p$, reduce the base (i.e., $a$) modulo $p$ and the exponent (i.e., $x$) modulo $p-1$.
Proof of Fermat’s Little Theorem

To prove Fermat’s Little Theorem, we first prove the following lemma.

**Lemma:** If \( n \) is an integer and \( a \in \mathbb{Z}_n^* \), then \( a \cdot k_1 \equiv a \cdot k_2 \mod n \) if and only if \( k_1 \equiv k_2 \mod n \).

**Proof:** Suppose \( k_1 a \equiv k_2 a \). Since \( a \in \mathbb{Z}_n^* \), there exists an inverse \( a^{-1} \in \mathbb{Z}_n^* \) such that \( a \cdot a^{-1} \equiv 1 \mod n \).

Therefore, \( (k_1 a) \cdot a^{-1} \equiv (k_2 a) \cdot a^{-1} \mod n \). But

\[
(k_1 a) \cdot a^{-1} = k_1 (a \cdot a^{-1}) \equiv k_1 \mod p
\]

and

\[
(k_2 a) \cdot a^{-1} = k_2 (a \cdot a^{-1}) \equiv k_2 \mod p;
\]

hence, it follows that \( k_1 \equiv k_2 \mod p \), as desired.
Proof of Fermat's Little Theorem

Fermat's Little Theorem: Let $p$ be a prime. Then for every $a \in \mathbb{Z}_p^*$, we have $a^{p-1} \equiv 1 \mod p$.

Proof: Consider the product $a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \mod p$.

By the lemma on the previous slide, it follows that the above product is congruent to $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$.

(Indeed, it is clearly a product of $p-1$ numbers from $\mathbb{Z}_p^*$; if these numbers aren't distinct, then we obtain an immediate contradiction.)

In other words, we have that $a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$.

Rearranging the left-hand side, we get $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$.

Thus, a second application of the lemma shows that $a^{p-1} \equiv 1 \mod p$. □
Generating random (probable) primes

- **Goal:** Generate a random \( n \)-bit prime
  - **Step 1:** Choose \( n \in_R [2^n+1, 2^{n+1}-1] \)
  - **Step 2:** Check if \( 2^{n-1} \equiv 1 \pmod{n} \)
    - If so, output \( n \); otherwise, go to Step 1

- If \( n \) is prime, then \( \Pr[2^{n-1} \equiv 1] = 1 \)
- If \( n \) is not prime, then \( \Pr[2^{n-1} \equiv 1] \) is “small”
  - Unless you get unlucky and \( n \) is a Carmichael number…
Chinese Remainder Theorem: Let $n_1, n_2, \ldots, n_k$ be positive integers with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$, and let $N = n_1 \cdot n_2 \cdots n_k$.

Then the system of congruence relations

\[
x \equiv c_1 \mod n_1 \\
\vdots \\
x \equiv c_k \mod n_k
\]

has a unique solution in $\mathbb{Z}_N$.

For each $i = 1, \ldots, k$, set $y_i = (N/n_i)^{-1} \mod n_i$ and $z_i = (N/n_i) \cdot y_i \mod N$.

The unique solution is $x \equiv \sum z_i \cdot c_i \mod N$. 

$z_i \equiv 1 \mod n_i$, $z_i \equiv 0 \mod n_j$ when $i \neq j$. 

Ryan Henry
Euler's phi function

**Defn:** Let \( n \) be a positive integer. Then Euler's phi function is \( \varphi(n) = |\mathbb{Z}_n^*| \). In particular, Euler's phi function of \( n \) indicates the number of positive integer less than and relatively prime to \( n \).

- If \( p \) is prime, then \( \varphi(p) = p-1 \)
- If \( p \) is prime, then \( \varphi(p^2) = p(p-1) \)
- If \( p \) is prime, then \( \varphi(p^k) = p^{k-1}(p-1) \)
- If \( p \) and \( q \) are distinct prime, then \( \varphi(p\cdot q) = p(q-1) \)
- If \( n = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k} \), then \( \varphi(n) = p_1^{e_1-1}(p_1-1) p_2^{e_2-1}(p_2-1) \cdots p_k^{e_k-1}(p_k-1) \)

**Thm (Fermat restatement):** If \( p \) is prime, then \( \forall a \in \mathbb{Z}_p^* \), \( a^{\varphi(p)} \equiv 1 \mod p \).
Euler's Theorem

Generalization of Fermat's Little Theorem

**Euler's Theorem**: For any integer \( n > 1 \) and \( a \in \mathbb{Z}_n^* \), \( a^{\varphi(n)} \equiv 1 \mod n \).

- \( 3^4 \equiv ? \mod 10 \)
- \( 84^{40} \equiv ? \mod 100 \) (since \( \varphi(100) = 5 \cdot (5-1) \cdot 2 \cdot (2-1) = 40 \))
- \( 79^{441} \equiv 79 \mod 100 \) (since \( 441 = 11 \cdot \varphi(100) + 1 \))
- The last two digits of \( 103^{81} \) are 01 (since \( 103^{81} \equiv 3 \mod 100 \))

**Trick**: To compute \( a^x \mod n \), reduce the base (i.e., \( a \)) modulo \( n \) and the exponent (i.e., \( x \)) modulo \( \varphi(n) \).
That's all for today, folks!