COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/
Definition: Divisor

Let $m \neq 0$ and $n, m \in \mathbb{Z}$, then $m$ divides $n$ if there exists a $q \in \mathbb{Z}$ such that $n = mq$.

We then also say that $n$ is a multiple of $q$.

We write $d | a$ and say $d$ divides $a$. 
Rules

\[ m \mid n \iff n \% m = 0 \] (1)

\[ n \mid 0 \land n \mid n \quad \text{for } n \neq 0 \] (2)

\[ m \mid n \Rightarrow -m \mid n \land m \mid -n \] (3)

\[ 1 \mid n \quad \text{for all } n \] (4)

\[ m \mid n \land n \neq 0 \Rightarrow |m| \leq |n| \] (5)

\[ n \mid 1 \Rightarrow |n| = 1 \] (6)
More Rules

\[ m | n \land n | m \Rightarrow n = m \lor n = -m \quad (7) \]

\[ m | n \iff lm | ln \quad \text{if } l \neq 0 \quad (8) \]

\[ m | n_1 \land m | n_2 \Rightarrow m | (l_1 n_1 + l_2 n_2) \quad \text{for all } l_1, l_2 \quad (9) \]

\[ m_1 | n_1 \land m_2 | n_2 \Rightarrow m_1 m_2 | n_1 n_2 \quad (10) \]
Definition: Prime Numbers

Let $\tau(n)$ be the number of positive divisors for $n \in \mathbb{N}$.

A prime number $p$ is a natural number with exactly two positive divisors ($1|p$ and $p|p$):

$$\tau(p) = 2.$$ (11)
Fundamental Theorem of Arithmetic

Every positive integer can be represented in exactly one way (modulo permutations) as a product of zero or more primes.
Greatest Common Divisor

d = \text{GCD}(a, b) \text{ if } d \in \mathbb{N} \text{ is the largest number such that } d | a \text{ and } d | b.
Euclidean Algorithm

unsigned int gcd(unsigned int a, unsigned int b) {
    unsigned int g = b;
    while (a > 0) {
        g = a;
        a = b % a;
        b = g;
    }
    return g;
}
Definition: Coprime

Two numbers $a, b \in \mathbb{Z}$ are called coprime, relatively prime or strangers if $GCD(a, b) = 1$. 
Multiplicative Functions

A function $f : \mathbb{Z} \rightarrow \mathbb{C}$ is called \textbf{multiplicative} if

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$$ \hspace{1cm} (12)

for all coprime numbers $n_1, n_2 \in \mathbb{N}$. 
Product of Infinite Series

If $f : \mathbb{Z} \to \mathbb{C}$ multiplicative and $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent, then:

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \sum_{v=0}^{\infty} f(p^v).$$  (13)

(using fundamental theorem of arithmetic).
Riemann Zeta Function

ζ : \mathbb{C} \rightarrow \mathbb{C} \text{ is for } Re \ s > 1 \text{ defined as:}

\[ \zeta(s) : = \sum_{n=1}^{\infty} n^{-s} \quad (14) \]

\[ = \prod \sum_{p} p^{-sv} \quad (15) \]

\[ = \prod_{p} (1 - p^{-s})^{-1}. \quad (16) \]

Proof: Using product of infinite series and summation of geometric series.
Euclid

“There are infinitely many primes.”

Non-standard Proof:

$$\zeta(2) = \sum_{n \in \mathbb{N}} n^{-2} = \frac{1}{6}\pi^2 \notin \mathbb{Q}.$$  \hspace{1cm} (17)
Modular Arithmetic

- \( a = a + (b \cdot n) \mod n \) for \( a, b \in \mathbb{Z}, n \in \mathbb{N} \)

- \( a \cdot b \equiv (a \mod n) \cdot (b \mod n) \mod n \)

We call the resulting ring \( \mathbb{Z}_n \).

For \( p \) prime, \( \mathbb{Z}_p \equiv \mathbb{F}_p \) is a field.
Modular Exponentiation (1/2)

How to calculate \( a^{14} \mod n \)?

1. \( a_1 \equiv a \mod n \)
2. \( a_2 \equiv a_1 \cdot a_1 \mod n \)
3. \( a_4 \equiv a_2 \cdot a_2 \mod n \)
4. \( a_8 \equiv a_4 \cdot a_4 \mod n \)
5. \( a_{12} \equiv a_8 \cdot a_4 \mod n \)
6. \( a_{14} \equiv a_{12} \cdot a_2 \mod n \)
Modular Exponentiation (2/2)

How to calculate $a^{14} \mod n$ in parallel?

1. $a_1 \equiv a \mod n$

2. $a_2 \equiv a_1 \cdot a_1 \mod n$

3. $a_3 \equiv a_1 \cdot a_2 \mod n$ and $a_4 \equiv a_2 \cdot a_2 \mod n$

4. $a_7 \equiv a_3 \cdot a_4 \mod n$

5. $a_{14} \equiv a_7 \cdot a_7 \mod n$
Inverses \ mod \ n

Given \( a \in \mathbb{Z}_n \), find \( x \in \mathbb{Z}_n \) such that

\[ a \cdot x \equiv 1 \ \text{mod} \ n. \quad (18) \]

We also write

\[ a^{-1} \equiv x \ \text{mod} \ n. \quad (19) \]

\( a^{-1} \) exists \ mod \ n if \( a \) and \( n \) are coprime.
Computing Inverses \( \mod n \)

Extended Euclidean algorithm finds \( x \) and \( y \) in

\[
a x + b y = \text{GCD}(a, b).
\]  \hspace{1cm} (20)

If \( a \) and \( b \) are coprime, then

\[
a x + b y = 1
\]  \hspace{1cm} (21)

\[
\Rightarrow a x \equiv 1 \mod b
\]  \hspace{1cm} (22)

\[
\Rightarrow a^{-1} \equiv x \mod n
\]  \hspace{1cm} (23)
Extended Euclidean Algorithm

fun extended_gcd(a, b)
    if a mod b = 0
        (0, 1, b)
    else let
        (x, y, g) = extended_gcd(b, a mod b)
    in
        (y, x - y * (a div b), g)
end
Homework

Either:

- Learn about functional programming, or
- Understand Schneier’s version on pages 246-248
Fermat’s Little Theorem

Let \( p \) be prime. Then

\[ a^p \equiv a \pmod{p} \tag{24} \]

for any \( a \). If \( p \nmid a \) then

\[ a^{p-1} \equiv 1 \pmod{p} \tag{25} \]
Euler’s Totient Function

\[ \phi_\alpha(n) := \# \left\{ (l_1, \ldots, l_\alpha) \in \{1, \ldots, n\}^\alpha : GCD(l_1, \ldots, l_\alpha, n) = 1 \right\} \]  \hspace{1cm} (26)

In particular \( \phi(n) := \phi_1(n) \) is the number of natural numbers smaller than \( n \) that are coprime to \( n \).
Computing Euler’s Totient Function

- $\phi(p) = p - 1$.
- $\phi(p^j) = p^{j-1} \cdot (p - 1)$.
- $\phi(n)$ is multiplicative.
Euler’s Theorem

Let $a, m \in \mathbb{N}$ be coprime. Then

$$a^{\phi(m)} \equiv 1 \mod m.$$  (27)
Factoring

I have nothing to do. So I'm trying to calculate the prime factors of the time each minute before it changes.

It was easy when I started at 1:00, but with each hour the number gets bigger. I wonder how long I can keep up.

Beep

Hey!

Think fast.
Factoring

• Factoring is assumed to be a hard problem.

• If not, a lot of cryptography breaks down.

• Complexity has not been established, but is likely not in $P$ or $NP$.

• The hardest problem is factoring products of two randomly-chosen primes of about the same size, but not too close.
Evidence of Complexity of Factoring

- General number field sieve for \( b \)-bit number has complexity

\[
O \left( \exp \left( \left( \frac{64}{9} b^{\frac{1}{3}} \log b^{\frac{2}{3}} \right) \right) \right).
\]

- RSA 640 has been factored, RSA-704 is still pending.
Prime Number Generation

• Factoring is hard

⇒ Cannot generate primes efficiently by factoring

• Use statistical tests:
  – For a *random* number $t$, non-primes pass with probability $1 - p$

⇒ Number passing $n$ tests is prime with probability $1 - p^n$. 
Lehmann

1. Choose a random number $a$ less than $p$.

2. Calculate $t \equiv a^{(p-1)/2} \mod p$.

3. If $t \neq \pm 1 \mod p$ then $p$ is not prime.

4. Otherwise the likelihood that $p$ is not prime is no more than 50%.
Rabin-Miller

Calculate \( m \) such that \( p = 1 + 2^b \cdot m \) using the largest \( b \) with \( 2^b | p - 1 \).

1. Choose a random positive number \( a \neq 1 \) less than \( p \).
2. Set \( j = 0 \) and \( z \equiv a^m \mod p \)
3. If \( z = 1 \) or \( z = p - 1 \) then \( p \) maybe prime.
4. If \( j > 0 \) and \( z = 1 \), then \( p \) is not prime.
5. Set \( j = j + 1 \). If \( j < b \) and \( z \neq p - 1 \) set \( z \equiv z^2 \mod p \)
   and go back to step 4.
6. If \( j = b \) and \( z \neq p - 1 \) then \( p \) is not prime.
Prime Number Generation

1. Choose a random $n$-bit number $p$.

2. Set the high-order and low-order bit to 1.

3. Check that $p$ is not divisible by any small primes (3, 5, 7, 11).


Naturally, step 3 is optional, but generally cheaper than Rabin-Miller.
Discrete Logarithms

Given \( a, b \in \mathbb{Z}_n \), find \( x \in \mathbb{Z}_n \) such that

\[ a^x \equiv b \pmod{n}. \] (29)

We also write

\[ \log_a b \equiv x \pmod{n}. \] (30)
Questions

?
**Problem**

Show that:

\[ m \mid n_1 \land m \mid n_2 \Rightarrow m \mid (l_1 n_1 + l_2 n_2) \quad \text{for all } l_1, l_2 \quad (31) \]

\[ m_1 \mid n_1 \land m_2 \mid n_2 \Rightarrow m_1 m_2 \mid n_1 n_2 \quad (32) \]
Problem

Find values for $a$, $b$ and $m$ such that there is no $x$ with

$$\log_a b \equiv x \mod n.$$  \hspace{1cm} (33)