Prime Numbers

Definition: An integer \( p > 1 \) is a prime if and only if its only positive integer divisors are 1 and \( p \).

Fact: Any integer \( a > 1 \) has a unique representation as a product of its prime divisors

\[
a = \prod_{i=1}^{t} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}
\]

where \( p_1 < p_2 < \cdots < p_t \) and each \( e_i \) is a positive integer.

Some first primes: 2,3,5,7,11,13,17,... For more primes, see:

www.utm.edu/research/primes/

Composite (non-prime) numbers and their factorisations:

\( 18 = 2 \times 3^2 \), \( 27 = 3^3 \), \( 42 = 2 \times 3 \times 7 \), \( 84773093 = 8887 \times 9539 \)
Euclid’s Algorithm

Given two positive integers and their representations as products of prime powers, it would be easy to extract from them the maximum set of common prime powers.

For example gcd(18, 42) = gcd(2×3², 2×3×7) = 2×3 = 6.

However, factoring integers is not an easy task.

Euclid’s algorithm is an efficient algorithm for finding the gcd of two integers. It is based on the following fact:

Let a > b. Then gcd(a, b) = gcd(a mod b, b).

Example: gcd(42, 18) = gcd(6, 18) = 6.

Example: gcd(595, 408) = gcd(187, 408) = gcd(187, 34) = gcd(17, 34) = 17.

Slowest case: Fibonacci sequence 1, 2, 3, 5, 8, 13, 21, ..., Fₙ = Fₙ₋₁ + Fₙ₋₂.

For example it takes 5 iterations to compute gcd(21, 13); in general it takes n-2 iterations to compute gcd(Fₙ, Fₙ₋₁).

Extended Euclidean Algorithm

and computing a modular inverse

Fact: Given two positive integers a and b there are integers u and v such that

\[ u×a + v×b = \text{gcd}(a, b) \]

In particular, if \( \text{gcd}(a, b) = 1 \), there is a positive integer \( u \) such that

\[ u×a = 1 \mod b, \]

and similarly, there is a positive integer \( v \) such that

\[ v×b = 1 \mod a. \]

\( u \) and \( v \) can be computed using the Extended Euclidean Algorithm, which iteratively finds integers \( r_i \), \( u_i \), and \( v_i \) such that

\[ r_i - q_i×r_{i-1} = r_{i-2} \quad \text{and} \quad u_i×a + v_i×b = r_i \]

\[ u_i = u_{i-2} - q_i×u_{i-1} \quad \text{and} \quad v_i = v_{i-2} - q_i×v_{i-1} \]

The index \( i = n \) for which \( r_n = \text{gcd}(a, b) \) gives \( u_n = u \) and \( v_n = v \).
### Extended Euclidean Algorithm: Example

\[ \text{gcd}(595, 408) = 17 = u \times 595 + v \times 408 \]

<table>
<thead>
<tr>
<th>( i )</th>
<th>( q_i )</th>
<th>( r_i )</th>
<th>( u_i )</th>
<th>( v_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>-</td>
<td>595</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>-</td>
<td>408</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>187</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>34</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>17</td>
<td>11</td>
<td>-16</td>
</tr>
</tbody>
</table>

### Extended Euclidean Algorithm: Examples

\[ \text{gcd}(595, 408) = 17 = 11 \times 595 + (-16) \times 408 \]
\[ = -397 \times 595 + 579 \times 408 \]

We get \( 11 \times 595 = 17 \pmod{408} \)
and \( 579 \times 408 = 17 \pmod{595} \)

If \( \text{gcd}(a,b) = 1 \), this algorithm gives modular inverses.

Example: \( 557 \times 797 = 1 \pmod{1047} \)
that is \( 557 = 797^{-1} \pmod{1047} \)

If \( \text{gcd}(a,b) = 1 \), the integers \( a \) and \( b \) are said to be coprime.
Computing multiplicative inverse: Example

\[ \text{gcd}(1047, 797) = 1 = u \times 797 + v \times 1047 \]

<table>
<thead>
<tr>
<th>( i )</th>
<th>( q_i )</th>
<th>( r_i )</th>
<th>( u_i )</th>
<th>( v_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>-</td>
<td>1047</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>-1</td>
<td>-</td>
<td>797</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>250</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>47</td>
<td>4</td>
<td>-3</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>15</td>
<td>-21</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>67</td>
<td>-51</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>1</td>
<td>-490</td>
<td>373</td>
</tr>
</tbody>
</table>

Chinese Remainder Theorem (two moduli)

Problem: Assume \( m_1 \) and \( m_2 \) are coprime. Given \( x_1 \) and \( x_2 \), how to find \( 0 \leq x < m_1 \cdot m_2 \) such that

\[ x = x_1 \text{ mod } m_1 \]
\[ x = x_2 \text{ mod } m_2 \]

Solution: Use the Extended Euclidean Algorithm to find \( u \) and \( v \) such that \( u \cdot m_1 + v \cdot m_2 = 1 \). Then

\[ x = x \cdot u \cdot m_1 + x \cdot v \cdot m_2 \]
\[ = (x_2 \cdot r \cdot m_2) \cdot u \cdot m_1 + (x_1 \cdot s \cdot m_1) \cdot v \cdot m_2 \]

It follows that

\[ x = x \text{ mod } (m_1 \cdot m_2) = (x_2 \cdot u \cdot m_1 + x_1 \cdot v \cdot m_2) \text{ mod } (m_1 \cdot m_2) \]
Chinese Remainder Theorem (general case)

Theorem: Assume $m_1$, $m_2$, ..., $m_t$ are mutually coprime. Denote $M = m_1 \times m_2 \times \ldots \times m_t$. Given $x_1$, $x_2$, ..., $x_t$ there exists a unique $x$, $0 < x < M$, such that

\[ x = x_1 \mod m_1 \]
\[ x = x_2 \mod m_2 \]
\[ \ldots \]
\[ x = x_t \mod m_t \]

$x$ can be computed as

\[ x = (x_1 \times u_1 \times M_1 + x_2 \times u_2 \times M_2 + \ldots + x_t \times u_t \times M_t) \mod M, \]

where $M_i = (m_1 \times m_2 \times \ldots \times m_t)/m_i$ and $u_i = M_i^{-1} \mod m_i$.

Chinese Remainder Theorem: Example

Assume $m_1 = 7$, $m_2 = 11$, $m_3 = 13$. Then $M = 1001$.

Compute $x$, $0 \leq x \leq 1000$ such that

\[ x = 5 \mod 7 \]
\[ x = 3 \mod 11 \]
\[ x = 10 \mod 13 \]

$M_1 = m_2m_3 = 143$; $M_2 = m_1m_3 = 91$; $M_3 = m_1m_2 = 77$

$u_1 = M_1^{-1} \mod m_1 = 143^{-1} \mod 7 = 3^{-1} \mod 7 = 5$; similarly $u_2 = M_2^{-1} \mod m_2 = 3^{-1} \mod 11 = 4$; $u_3 = (-1)^{-1} \mod 13 = -1$.

Then

\[ x = (5 \times 5 \times 143 + 3 \times 4 \times 91 + 10 \times (-1) \times 77) \mod 1001 = 894 \]
Euler’s Totient Function $\phi(n)$

Definition: Let $n > 1$ be integer. Then

$\phi(n) = \#\{ a | 0 < a < n, \gcd(a,n) = 1\}$, that is, $\phi(n)$ is the number of positive integers less than $n$ which are coprime with $n$.

For prime $p$, $\phi(p) = p - 1$. We set $\phi(1) = 1$.

For a prime power, we have $\phi(p^e) = p^{e-1}(p-1)$

Given $m, n$, $\gcd(m, n) = 1$, we have $\phi(m \times n) = \phi(m) \times \phi(n)$.

Now Euler’s totient function can be computed for any integer using its prime factorisation.

Example: $\phi(18) = \phi(2 \times 3^2) = \phi(2) \times \phi(3^2) = (2-1) \times (3-1) \times 3^1 = 6$,
that is, the number of invertible numbers modulo 18 is equal to 6. These numbers are: 1, 5, 7, 11, 13, 17.

Euler’s Theorem

$Z_n^* = \{a | 0 < a < n, \gcd(a, n) = 1\}$, and $\# Z_n^* = \phi(n)$

Euler’s Theorem: For any integers $n$ and $a$ such that $a \neq 0$ and $\gcd(a, n) = 1$ the following holds:

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

Fermat’s Theorem: For a prime $p$ and any integer $a$ such that $a \neq 0$ and $a$ is not a multiple of $p$ the following holds:

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