An Algorithm for Prime Factorization

Fact: If $a$ is the smallest number $> 1$ that divides $n$, then $a$ is prime.

Proof: By contradiction. (Left to the reader.)

- A multiset is like a set, except repetitions are allowed
  - $\{\{2, 2, 3, 3, 5\}\}$ is a multiset, not a set

### PF$(n)$: A prime factorization procedure

**Input:** $n \in N^+$

**Output:** PFS - a multiset of $n$’s prime factors

PFS := $\emptyset$

for $a = 2$ to $\sqrt{n}$ do
  if $a \mid n$ then PFS := PF($n/a$) $\cup\{\{a\}\}$ return PFS

if PFS = $\emptyset$ then PFS := $\{\{n\}\}$  [n is prime]

**Example:** PF(7007) = $\{\{7\}\} \cup$ PF(1001)

= $\{\{7, 7\}\} \cup$ PF(143)

= $\{\{7, 7, 11\}\} \cup$ PF(13)

= $\{\{7, 7, 11, 13\}\}$. 
The Complexity of Factoring

Algorithm PF runs in exponential time:

- We’re checking every number up to $\sqrt{n}$

Can we do better?

- We don’t know.
- Modern-day cryptography implicitly depends on the fact that we can’t!
How Many Primes Are There?

**Theorem 4:** [Euclid] There are infinitely many primes.

**Proof:** By contradiction.

- Suppose that there are only finitely many primes: $p_1, \ldots, p_n$.
- Consider $q = p_1 \times \cdots \times p_n + 1$.
- Clearly $q > p_1, \ldots, p_n$, so it can’t be prime.
- So $q$ must have a prime factor, which must be one of $p_1, \ldots, p_n$ (since these are the only primes).
- Suppose it is $p_i$.
  - Then $p_i \mid q$ and $p_i \mid p_1 \times \cdots \times p_n$.
  - So $p_i \mid (q - p_1 \times \cdots \times p_n)$; i.e., $p_i \mid 1$ (Corollary 1).
  - Contradiction!

Largest currently-known prime (as of 5/04):
- $2^{24036583} - 1$: 7235733 digits
- Check [www.utm.edu/research/primes](http://www.utm.edu/research/primes)

Primes of the form $2^p - 1$ where $p$ is prime are called **Mersenne primes**.

- Search for large primes focuses on Mersenne primes
The distribution of primes

There are quite a few primes out there:

• Roughly one in every \( \log(n) \) numbers is prime

Formally: let \( \pi(n) \) be the number of primes \( \leq n \):

**Prime Number Theorem Theorem:** \( \pi(n) \sim n/\log(n) \);
that is,

\[
\lim_{n \to \infty} \frac{\pi(n)}{n/\log(n)} = 1
\]

Why is this important?

• Cryptosystems like RSA use a secret key that is the product of two large (100-digit) primes.

• How do you find two large primes?
  - Roughly one of every 100 100-digit numbers is prime
  - To find a 100-digit prime:
    * Keep choosing odd numbers at random
    * Check if they are prime (using fast randomized primality test)
    * Keep trying until you find one
    * Roughly 100 attempts should do it
(Some) Open Problems Involving Primes

- Are there infinitely many Mersenne primes?
- Goldbach’s Conjecture: every even number greater than 2 is the sum of two primes.
  - E.g., $6 = 3 + 3$, $20 = 17 + 3$, $28 = 17 + 11$
  - This has been checked out to $6 \times 10^{16}$ (as of 2003)
  - Every sufficiently large integer ($> 10^{43,000}$) is the sum of four primes
- Two prime numbers that differ by two are twin primes
  - E.g.: (3,5), (5,7), (11,13), (17,19), (41,43)
  - also 4, 648, 619, 711, 505 \times 2^{60,000} \pm 1!

Are there infinitely many twin primes?

All these conjectures are believed to be true, but no one has proved them.
Greatest Common Divisor (gcd)

**Definition:** For $a \in \mathbb{Z}$ let $D(a) = \{k \in \mathbb{N} : k \mid a\}$
- $D(a) = \{\text{divisors of } a\}$.

**Claim.** $|D(a)| < \infty$ if (and only if) $a \neq 0$.

**Proof:** If $a \neq 0$ and $k \mid a$, then $0 < k < a$.

**Definition:** For $a, b \in \mathbb{Z}$, $CD(a, b) = D(a) \cap D(b)$ is the set of common divisors of $a, b$.

**Definition:** The *greatest common divisor* of $a$ and $b$ is

$$\gcd(a, b) = \max(CD(a, b)).$$

**Examples:**
- $\gcd(6, 9) = 3$
- $\gcd(13, 100) = 1$
- $\gcd(6, 45) = 3$

**Def.:** $a$ and $b$ are *relatively prime* if $\gcd(a, b) = 1$.
- **Example:** 4 and 9 are relatively prime.
- Two numbers are relatively prime iff they have no common prime factors.

Efficient computation of $\gcd(a, b)$ lies at the heart of commercial cryptography.
Least Common Multiple (lcm)

Definition: The least common multiple of $a, b \in N^+$, \( \text{lcm}(a, b) \), is the smallest $n \in N^+$ such that $a \mid n$ and $b \mid n$.

- Formally, $M(a) = \{ka \mid k \in N\}$ – the multiples of $a$
- Define $CM(a, b) = M(a) \cap M(b)$ – the common multiples of $a$ and $b$
- $\text{lcm}(a, b) = \min(CM(a, b))$
- Examples: $\text{lcm}(4, 9) = 36$, $\text{lcm}(4, 10) = 20$. 
Computing the GCD

There is a method for calculating the gcd that goes back to Euclid:

• **Recall:** if $n > m$ and $q$ divides both $n$ and $m$, then $q$ divides $n - m$ and $n + m$.

Therefore $\gcd(n, m) = \gcd(m, n - m)$.

• Proof: Show $CD(m, n) = CD(m, n - m)$; i.e., that $q$ divides both $n$ and $m$ iff $q$ divides both $m$ and $n - m$. (If $q$ divides $n$ and $m$, then $q$ divides $n - m$ by the argument above. If $q$ divides $m$ and $n - m$, then $q$ divides $m + (n - m) = n$.)

• This allows us to reduce the gcd computation to a simpler case.

We can do even better:

- $\gcd(n, m) = \gcd(m, n - m) = \gcd(m, n - 2m) = \ldots$
- keep going as long as $n - qm \geq 0$ — $\lceil n/m \rceil$ steps

Consider $\gcd(6, 45)$:

- $\lceil 45/6 \rceil = 7$; remainder is 3 ($45 \equiv 3 \pmod{6}$)
- $\gcd(6, 45) = \gcd(6, 45 - 7 \times 6) = \gcd(6, 3) = 3$
We can keep this up this procedure to compute gcd($n_1, n_2$):

- If $n_1 \geq n_2$, write $n_1$ as $q_1n_2 + r_1$, where $0 \leq r_1 < n_2$
  - $q_1 = \lfloor n_1/n_2 \rfloor$
- $\gcd(n_1, n_2) = \gcd(r_1, n_2)$; $r_1 = n_1 \mod n_2$
- Now $r_1 < n_2$, so switch their roles:
- $n_2 = q_2r_1 + r_2$, where $0 \leq r_2 < r_1$
- $\gcd(r_1, n_2) = \gcd(r_1, r_2)$
- Notice that $\max(n_1, n_2) > \max(r_1, n_2) > \max(r_1, r_2)$
- Keep going until we have a remainder of 0 (i.e., something of the form $\gcd(r_k, 0)$ or $(\gcd(0, r_k)$)
  - This is bound to happen sooner or later
Euclid’s Algorithm

**Input** $m, n$  \quad [m, n$ natural numbers, \(m \geq n\)]  
\[\text{num} \leftarrow m; \text{denom} \leftarrow n\]  \quad [Initialize num and denom]  
**repeat** until denom = 0  
\[q \leftarrow \lfloor \text{num}/\text{denom} \rfloor\]  
\[\text{rem} \leftarrow \text{num} - (q \times \text{denom})\]  \quad [num mod denom = rem]  
\[\text{num} \leftarrow \text{denom}\]  \quad [New num]  
\[\text{denom} \leftarrow \text{rem}\]  \quad [New denom; note \(num \geq denom\)]  
**endrepeat**  
**Output** num [num = gcd(m, n)]

Example: gcd(84, 33)

Iteration 1: num = 84, denom = 33, \(q = 2\), rem = 18  
Iteration 2: num = 33, denom = 18, \(q = 1\), rem = 15  
Iteration 3: num = 18, denom = 15, \(q = 1\), rem = 3  
Iteration 4: num = 15, denom = 3, \(q = 5\), rem = 0  
Iteration 5: num = 3, denom = 0 \(\Rightarrow\) gcd(84, 33) = 3  

gcd(84, 33) = gcd(33, 18) = gcd(18, 15) = gcd(15, 3) = gcd(3, 0) = 3
Euclid’s Algorithm: Correctness

How do we know this works?

• We have two loop invariants, which are true each time we start the loop:

  ○ $\gcd(m, n) = \gcd(num, denom)$
  ○ $num \geq denom$

• At the end, $denom = 0$, so $\gcd(num, denom) = num$. 
Euclid’s Algorithm: Complexity

Input $m, n$ [m, n natural numbers, $m \geq n$]
num ← $m$; denom ← $n$  [Initialize num and denom]
repeat until denom = 0
    $q \leftarrow \lfloor num/denom \rfloor$
    rem ← num − ($q \times denom$)
    num ← denom  [New num]
    denom ← rem  [New denom; note num $\geq$ denom]
endrepeat
Output num [num = gcd($m, n$)]

How many times do we go through the loop in the Euclidean algorithm:

- Best case: Easy. Never!
- Average case: Too hard
- Worst case: Can’t answer this exactly, but we can get a good upper bound.
  - See how fast denom goes down in each iteration.
Claim: After two iterations, \( denom \) is halved:

- Recall \( num = q \times denom + rem \). Use \( denom' \) and \( denom'' \) to denote value of \( denom \) after 1 and 2 iterations. Two cases:

  1. \( rem \leq denom/2 \Rightarrow denom' \leq denom/2 \) and \( denom'' < denom/2 \).

  2. \( rem > denom/2 \). But then \( num' = denom \), \( denom' = rem \). At next iteration, \( q = 1 \), and \( denom'' = rem' = num' - denom' < denom/2 \).

- How long until \( denom \) is \( \leq 1 \)?
  
  - \( < 2 \log_2(m) \) steps!

- After at most \( 2 \log_2(m) \) steps, \( denom = 0 \).
The Extended Euclidean Algorithm

**Theorem 5:** For $a, b \in \mathbb{N}$, not both 0, we can compute $s, t \in \mathbb{Z}$ such that

$$\gcd(a, b) = sa + tb.$$ 

- **Example:** $\gcd(9, 4) = 1 = 1 \cdot 9 + (-2) \cdot 4$.

**Proof:** By strong induction on $\max(a, b)$. Suppose without loss of generality $a \leq b$.

- If $\max(a, b) = 1$, then must have $b = 1$, $\gcd(a, b) = 1$
  
  $\circ \gcd(a, b) = 0 \cdot a + 1 \cdot b$.

- If $\max(a, b) > 1$, there are three cases:
  
  $\circ$ If $a = 0$, then $\gcd(a, b) = b = 0 \cdot a + 1 \cdot b$
  
  $\circ$ If $a = b$, then $\gcd(a, b) = a = 1 \cdot a + 0 \cdot b$
  
  $\circ$ If $0 < a < b$, then $\gcd(a, b) = \gcd(a, b - a)$. Moreover, $b = \max(a, b) > \max(a, b - a)$. Thus, by IH, we can compute $s, t$ such that

  $$\gcd(a, b) = \gcd(a, a-b) = sa+t(b-a) = (s-t)a+tb.$$ 

**Note:** this computation basically follows the “recipe” of Euclid’s algorithm.
Example

Recall that $\gcd(84, 33) = \gcd(33, 18) = \gcd(18, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$

We work backwards to write 3 as a linear combination of 84 and 33:

$3 = 18 - 15$

[Now 3 is a linear combination of 18 and 15]

$= 18 - (33 - 18)$

$= 2(18) - 33$

[Now 3 is a linear combination of 18 and 33]

$= 2(84 - 2 \times 33)) - 33$

$= 2 \times 84 - 5 \times 33$

[Now 3 is a linear combination of 84 and 33]
Some Consequences

**Corollary 2:** If \( a \) and \( b \) are relatively prime, then there exist \( s \) and \( t \) such that \( as + bt = 1 \).

**Corollary 3:** If \( \gcd(a, b) = 1 \) and \( a \mid bc \), then \( a \mid c \).

**Proof:**

- Exist \( s, t \in \mathbb{Z} \) such that \( sa + tb = 1 \)
- Multiply both sides by \( c \): \( sac + tbc = c \)
- Since \( a \mid bc \), \( a \mid sac + tbc \), so \( a \mid c \)

**Corollary 4:** If \( p \) is prime and \( p \mid \prod_{i=1}^{n} a_i \), then \( p \mid a_i \) for some \( 1 \leq i \leq n \).

**Proof:** By induction on \( n \):

- If \( n = 1 \): trivial.

Suppose the result holds for \( n \leq N \) and \( p \mid \prod_{i=1}^{N+1} a_i \).

- Note that \( p \mid \prod_{i=1}^{N+1} a_i = (\prod_{i=1}^{N} a_i)a_{N+1} \).
- If \( p \mid a_{N+1} \) we are done.
- If not, \( \gcd(p, a_{N+1}) = 1 \).
- By Corollary 3, \( p \mid \prod_{i=1}^{N} a_i \)
- By the IH, \( p \mid a_i \) for some \( 1 \leq i \leq N \).
The Fundamental Theorem of Arithmetic, II

**Theorem 3:** Every $n > 1$ can be represented uniquely as a product of primes, written in nondecreasing size.

**Proof:** Still need to prove uniqueness. We do it by strong induction.

- **Base case:** Obvious if $n = 2$.

Inductive step. Suppose OK for $n' < n$.

- Suppose that $n = \Pi_{i=1}^{s} p_i = \Pi_{j=1}^{r} q_j$.
- $p_1 \mid \Pi_{j=1}^{r} q_j$, so by Corollary 4, $p_1 \mid q_j$ for some $j$.
- But then $p_1 = q_j$, since both $p_1$ and $q_j$ are prime.
- But then $n/p_1 = p_2 \cdots p_s = q_1 \cdots q_{j-1}q_{j+1} \cdots q_r$
- Result now follows from I.H.
Characterizing the GCD and LCM

**Theorem 6:** Suppose \( a = \Pi_{i=1}^{n} p_i^{\alpha_i} \) and \( b = \Pi_{i=1}^{n} p_i^{\beta_i} \), where \( p_i \) are primes and \( \alpha_i, \beta_i \in \mathbb{N} \).

- Some \( \alpha_i \)’s, \( \beta_i \)’s could be 0.

Then
\[
\text{gcd}(a, b) = \Pi_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}
\]
\[
\text{lcm}(a, b) = \Pi_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}
\]

**Proof:** For gcd, let \( c = \Pi_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)} \).
Clearly \( c \mid a \) and \( c \mid b \).

- Thus, \( c \) is a common divisor, so \( c \leq \text{gcd}(a, b) \).

If \( q^\gamma \mid \text{gcd}(a, b) \),

- must have \( q \in \{p_1, \ldots, p_n\} \)
  - Otherwise \( q \nmid a \) so \( q \nmid \text{gcd}(a, b) \) (likewise \( b \))

If \( q = p_i, q^\gamma \mid \text{gcd}(a, b) \), must have \( \gamma \leq \min(\alpha_i, \beta_i) \)
  - E.g., if \( \gamma > \alpha_i \), then \( p_i^{\gamma} \nmid a \)

- Thus, \( c \geq \text{gcd}(a, b) \).

Conclusion: \( c = \text{gcd}(a, b) \).
For lcm, let \( d = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)} \).

- Clearly \( a \mid d, \ b \mid d \), so \( d \) is a common multiple.
- Thus, \( d \geq \text{lcm}(a, b) \).

But if \( p_i^\delta \mid \text{lcm}(a, b) \), must have \( \delta \geq \max(\alpha_i, \beta_i) \).

- E.g., if \( \delta < \alpha_i \), then \( a \not\mid \text{lcm}(a, b) \).
- Thus, \( d \leq \text{lcm}(a, b) \).

Conclusion: \( d = \text{lcm}(a, b) \).

**Example:** \( 432 = 2^43^3 \), and \( 95256 = 2^33^57^2 \), so

- \( \gcd(95256, 432) = 2^33^3 = 216 \)
- \( \text{lcm}(95256, 432) = 2^43^57^2 = 190512 \).

**Corollary 5:** \( ab = \gcd(a, b) \cdot \text{lcm}(a, b) \)

**Proof:**

\[
\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta.
\]

**Example:** \( 4 \cdot 10 = 2 \cdot 20 = \gcd(4, 10) \cdot \text{lcm}(4, 10) \).