Elementary number theory

- **Why bother?** – When you hear the word Amazon do you think of a river in Brazil or of the internet commerce giant?

- **Def.** For $a, b \in \mathbb{Z}$, $a \neq 0$, a <u>divides</u> b (denoted $a \mid b$), if $\exists c \in \mathbb{Z}$ s.t. $b = ca$.

- More nomenclature: a is a *factor* of b, b is a *multiple* of a, $a \nmid b$.

- The integers divided by $d \in \mathbb{N}^+$ form a lattice $d\mathbb{Z}$:

- Q: How many integers in $[1, n]$ are divided by d?

- A: $\lfloor n/d \rfloor$.

Useful elementary result

- **Theorem.** For $a, b, c \in \mathbb{Z}$ we have:
  1. $a \mid b$ and $a \mid c \Rightarrow a \mid (b + c)$
  2. $a \mid b \Rightarrow a \mid (bc)$
  3. $a \mid b$ and $b \mid c \Rightarrow a \mid c$
- **Proof of 1.**

$$\begin{aligned} a \mid b &\Rightarrow \exists k \in \mathbb{Z} \text{ s.t. } b = ak \\ a \mid c &\Rightarrow \exists m \in \mathbb{Z} \text{ s.t. } c = am \\ &\Rightarrow b + c = ak + am = a(k + m) \\ &\Rightarrow a \mid b + c. \end{aligned}$$

Primes

- **Def.** $p \in \mathbb{N}$ is *prime* if $p > 1$ and $a \mid p$ implies $a = 1$ or $a = p$.
- $p > 1$ is prime if its only factors are 1 and itself.
- **Def.** $k \in \mathbb{N}$ is *composite* if $k > 1$ and k is not prime.
- If k is composite then $\exists a \in \mathbb{N}$, $1 < a < k$ s.t. $a \mid k$.
- Primes: $2, 3, 5, 7, 11, 13, \ldots$
- Composites: $4, 6, 8, 9, \ldots$
- **Primality testing.** How can we tell if $n \in \mathbb{N}$ is prime?
- The naive approach: check if $k \mid n$ for every $1 < k < n$.
- The complexity of this approach is *exponential* in the size of the input:
  - It takes $\log_2 n$ bits to describe n.
  - Checking if $k \mid n$ for any $k \in [2, n-1]$ requires $n - 2 = 2^{\log_2 n} - 2$ such tests.
- We can do significantly better.

Prime Factorization I

- **Theorem.** Any $n \in \mathbb{N}^+$ can be represented as a product of primes.
- Examples: $54 = 2 \cdot 3^3$, $100 = 2^2 \cdot 5^2$, $15 = 3 \cdot 5$.
- **Comments:**
  - This representation is in fact unique up to...
  - The uniqueness statement is the harder part of the fundamental theorem of arithmetic.
  - The product might be empty or have only one element.

Prime Factorization I

- **Theorem.** Any $n \in \mathbb{N}^+$ can be represented as a product of primes.
- **Proof.** By induction on n.
  - · The base of the induction is hidden in the aforementioned comments.
  - · Assuming any $k \leq n$ can be presented as a product of primes we want to factor $n + 1$.
  - · If $n + 1$ is prime then there is nothing to prove.
  - · Otherwise, $n + 1 = ab$ with $a, b \in \mathbb{N}$ and $1 < a, b < n + 1$.
  - · Thus, there exist primes $p_1, \ldots, p_i$ and $q_1, \ldots, q_j$ s.t.
  - · $a = p_1 \ldots p_i$ and $b = q_1 \ldots q_j$ and
  - · $n + 1 = p_1 \ldots p_i q_1 \ldots q_j$

A better primality test

- **Claim.** If n is a composite integer then n has a prime divisor $p \le \sqrt{n}$.
- **Proof.** $n = ab$ with $a, b \in \mathbb{N}$ and $1 < a, b < n$.
  - · Clearly, $a \le \sqrt{n}$ or $b \le \sqrt{n}$.
  - · WLOG (without loss of generality) $a \le \sqrt{n}$.
  - · $a = p_1 \ldots p_i$ where $p_j \le a \le \sqrt{n}$ are primes.
  - · $p_1 \mid a$ and $a \mid n$ so $p_1 \mid n$ and $p_1 \le \sqrt{n}$.
- **Corollary.** To test whether n is prime we only need to test if $k \mid n$ for any $2 \le k \le \sqrt{n}$.
- The number of "is factor?" tests are now reduced to roughly $\sqrt{n}$. Is it significant?
- Depends: $\sqrt{n} = 2^{0.5 \log_2 n}$.
- In fact, we only need to test if $p \mid n$ for every prime $p \le \sqrt{n}$.
- Does the last statement strike you as odd?
- Still, we can establish 101 is prime since 2, 3, 5 and 7 do not divide 101.

Prime Factorization II

PF(n): A prime factorization procedure
Input: $n \in \mathbb{N}^+$
Output: PFS - a list of n's prime factors

```
PFS := [n]
for i = 2 : √n
   if i | n
      PFS := [i] . PF(n/i)
      break
return PFS
```

- Example: PF(7007) = [7, PF(1001)] = [7, 7, PF(143)] = [7, 7, 11, PF(13)] = [7, 7, 11, 13].
- Can you identify a small (technical) bug in the program?
- Complexity wise, testing primality is easy (polynomial in the size of the input data) while prime factorization is difficult (it better be!).

The division algorithm

- **Theorem.** For $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, $d > 0$ there exist unique $q, r \in \mathbb{Z}$ s.t. $a = q \cdot d + r$ and $0 \leq r < d$.
- · d is the divisor
  · a is the dividend
  · q is the quotient
  · r is the remainder: $r = \underline{a \bmod d}$
  · $d \mid a$ if and only if $a \bmod d = 0$.
- · Example: dividing 101 by 11 gives a quotient of 9 and a remainder of 2 ($101 \bmod 11 = 2$).
  · Dividing 18 by 6 gives a quotient of 3 and a remainder of 0 ($18 \bmod 6 = 0$).
- **Proof.** Let $q = \lfloor a/d \rfloor$ and define $r = a - q \cdot d$. Then
  · $0 \leq a/d - \lfloor a/d \rfloor < 1 \quad \Longrightarrow \quad 0 \leq a - q \cdot d < d$.
  · So $a = q \cdot d + r$ with $q \in \mathbb{Z}$ and $0 \leq r < d$.
  · Uniqueness: suppose $q \cdot d + r = q' \cdot d + r'$ with $q', r' \in \mathbb{Z}$ and $0 \leq r' < d$.
  · It folows that $(q' - q)d = (r - r')$ with $-d < r - r' < d$.
  · The lhs is divisible by d so $r = r'$ and we're done.

How many primes are there?

- Suppose there was a finite number of primes: $p_1, \ldots p_n$.
- Let $N = 1 + \prod_1^n p_i$.
- For any i, $p_i \nmid N$ since $N \mod p_i = 1$.
- Yet N has a prime factorization so there have to be more primes.
- Let $\pi(n)$ be the numbers or primes $\leq n$.
- **The Prime Numbers Theorem.** $\pi(n) \sim n/\log(n)$, that is,
$$\lim_n \frac{\pi(n)}{n/\log(n)} = 1.$$
- Note that $a_n/b_n \to 1$ is not the same as $a_n - b_n \to 0$.

Greatest Common Divisor (gcd)

- For $a \in \mathbb{Z}$ let $D(a) = \{k \in \mathbb{N} : k \mid a\}$ (divisors of a).
- **Claim.** $|D(a)| < \infty$ if (and only if) $a \neq 0$.
- **Proof.**
  - · $k \in D(a)$ implies $a = kq$ for some $q \in \mathbb{Z}$, $q \neq 0$.
  - · $k = |a/q| \leq |a|$.
- For $a, b \in \mathbb{Z}$, let $CD(a, b) = D(a) \cap D(b)$ be the set of common divisors of a, b.
- Clearly $|CD(a, b)| < \infty$ if not both $a, b = 0$.
- **Def.** The *greatest common divisor* of a and b is: $\gcd(a, b) = \max CD(a, b)$.
- This is a constructive definition. Examples:
  - · gcd(6,9) = 3
  - · gcd(13,100) = 1
  - · gcd(4,9) = 1
- Efficient computation of $\gcd(a, b)$ lies at the heart of commercial cryptography (in particular the internet).

Euclid's Algorithm

- **Lemma.** If for $a, b, q, r \in \mathbb{Z}$, $a = bq + r$, then
$$\gcd(a, b) = \gcd(b, r).$$

- **Proof of lemma.**

  $k \in CD(a, b) \Rightarrow k \mid a - bq \Rightarrow k \mid r \Rightarrow k \in CD(b, r)$.

  $k \in CD(b, r) \Rightarrow k \mid bq + r \Rightarrow k \mid a \Rightarrow k \in CD(a, b)$.

  Thus,
$$CD(a, b) = CD(b, r).$$

- **Corollary.** $\gcd(a, b) = \gcd(b, a \bmod b)$.

- **Euclid's algorithm.** Upon input $a, b \in \mathbb{N}$:
  - Assuming $a \geq b$ and $a > 0$, let $r_0 = a$ and $r_1 = b$
  - As long as $r_i > 0$ let $r_{i+1} = r_{i-1} \bmod r_i$
  - Return r_n, the last nonvanishing r_i.

- Spelled Out: $r_0 = r_1 q_1 + r_2$ with $0 < r_2 < r_1$
  - $r_1 = r_2 q_2 + r_3$ with $0 < r_3 < r_2$

    $\vdots$
  - $r_{n-2} = q_{n-1} r_{n-1} + r_n$ with $0 < r_n < r_{n-1}$
  - $r_{n-1} = r_n q_n$

Euclid's Algorithm cont.

- When we stop we have:
- $\gcd(a, b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$
- Example. gcd(662,414)=?
  - $662 = 414 \cdot 1 + 248$
  - $414 = 248 \cdot 1 + 166$
  - $248 = 166 \cdot 1 + 82$
  - $166 = 82 \cdot 2 + 2$
  - $82 = 2 \cdot 41$
  - $\Rightarrow$ gcd(662,414) $= 2$

recursive_Euclid(a, b)
Input: $a \geq b \in \mathbb{N}$, $a > 0$
Output: $\gcd(a, b)$

```
if b = 0
    return a
else
    return recursive_Euclid(b, a mod b)
```

- What if $a < 0$ or $b < 0$?

Complexity of Euclid's Algorithm

- How do we know we will stop?
- The number of divisions is not more than $\min\{a, b\}$.
- This is typically *exponential* in the number of bits required to descibe the input.
- Recall: $r_{i-1} = r_i q_i + r_{i+1}$ with $q_i \in \mathbb{Z}$ and $0 \leq r_{i+1} < r_i$.
- Either $r_{i+1} \leq r_i/2$ or $r_{i+1} > r_i/2$.
- In the latter case, in $r_i = r_{i+1}q_{i+1} + r_{i+2}$, $q_{i+1} = 1$ and $r_{i+2} = r_i - r_{i+1} < r_i/2$.
- Either way, $r_{i+2} < r_i/2$, so every two steps reduce r_i by at least a factor of 2.
- The number of divisions is bounded by $2\log_2 n + 1$.
- Linear complexity.

Euclid's Extended Algorithm

- **Theorem.** For $a, b \in \mathbb{N}$, not both 0, there exist $s, t \in \mathbb{Z}$ s.t.
$$\gcd(a, b) = sa + tb.$$
- · Note that $\gcd(a, b) | sa + tb$ for all $s, t \in \mathbb{Z}$.
  · Example: $\gcd(9, 4) = 1 = 1 \cdot 9 + (-2) \cdot 4$.
- **Proof.** We will prove by induction on $0 \leq k \leq n$ that $\exists s_k, t_k \in \mathbb{Z}$ s.t.
$$s_k a + t_k b = r_k. \tag{1}$$
  · For $k = 0, 1$ this is obvious.
  · Assuming (1) holds for all $0 \leq k \leq m$ with $1 \leq m < n$, we want to show it holds for $k = m + 1$.
  · $r_{m-1} = q_m r_m + r_{m+1}$
  · $\Rightarrow (s_{m-1}a + t_{m-1}b) = q_m(s_m a + t_m b) + r_{m+1}$
  · $\Rightarrow (s_{m-1} - q_m s_m)a + (t_{m-1} - q_m t_m)b = r_{m+1}$
  · Let $s_{m+1} = s_{m-1} - q_m s_m$ and $t_{m+1} = t_{m-1} - q_m t_m$.
- Note that there is a recipe in the proof.

Corollaries

- **Lemma 1.** Let $a, b, c \in \mathbb{N}^+$ and suppose that $\gcd(a, b) = 1$ and that $a \mid bc$. Then $a \mid c$.
- **Proof.**
  - · $\exists s, t \in \mathbb{Z}$ s.t. $sa + tb = 1$
  - · $\Rightarrow sac + tbc = c$
  - · $\Rightarrow a \mid c$.
- $a, b \in \mathbb{Z}$ for which $\gcd(a, b) = 1$ are called *relatively primes* and they have no common prime factor.
- · Example: 4 and 9 are relatively primes.
  · $6 \mid 4 \cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$ – what's wrong?
- **Lemma 2.** If p is a prime and if for $a_i \in \mathbb{Z}$, $p \mid \prod_1^n a_i$, then $p \mid a_i$ for some $1 \leq i \leq n$.
- **Proof.** By induction on n ($n = 1$ is trivial).
  - · Assume the lemma holds for $1 \leq n \leq N$.
  - · $p \mid \prod_1^{N+1} a_i \Rightarrow p \mid (\prod_1^N a_i) a_{N+1}$.
  - · If $p \mid a_{N+1}$ we are done.
  - · Else, $\gcd(p, a_{N+1}) = 1$.
  - · Since $p \mid \prod_1^N a_i$, $p \mid a_i$ for some $1 \leq i \leq N$.

Fundamental Theorem of Arithmetic

- Every $n \in \mathbb{N}^+$ can be represented uniquely as a product of increasing primes.
- **Proof.** Only uniqueness is left to prove.
  - $\cdot$ Suppose $\exists n \in \mathbb{N}^+$ with two different prime factorizations.
  - $\cdot$ $n = \prod_1^s p_i = \prod_1^r q_j$.
  - $\cdot$ WLOG $p_i \neq q_j$ for all i, j.
  - $\cdot$ $p_1 \mid \prod_1^r q_j \Rightarrow p_i \mid q_j$ for some j.
  - $\cdot$ It follows that $p_1 = q_j$ which is a contradiction.
- **Corollary.** Suppose $a = \prod_1^n p_i^{\alpha_i}$ and $b = \prod_1^n p_i^{\beta_i}$, where p_i are primes and $\alpha_i, \beta_i \in \mathbb{N}$ (prime factorization). Then,

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}.$$

- **Proof.** Clearly, $\exists \gamma_i \in \mathbb{N}$ s.t. $\gcd(a, b) = \prod_1^n p_i^{\gamma_i} \prod_{n+1}^N p_i^{\gamma_i}$.
  - $\cdot$ $\gcd(a, b) \mid a \Rightarrow \forall i,\ \gamma_i \leq \alpha_i,\ (\alpha_{n+1} = \cdots = 0)$.
  - $\cdot$ Similarly, $\forall i \leq N$, $\gamma_i \leq \beta_i$, so $\gamma_i \leq \min(\alpha_i, \beta_i)$.
  - $\cdot$ Conversely, if $\exists i : \gamma_i < \min(\alpha_i, \beta_i)$ then

    $\gcd(a, b)p_i \mid a\ ,\ \gcd(a, b)p_i \mid b \Rightarrow$ contradiction.

Least Common Multiple (lcm)

- **Def.** The *least common multiple* of $a, b \in \mathbb{N}^+$, $\mathrm{lcm}(a, b)$, is the smallest $n \in \mathbb{N}^+$ s.t. $a \mid n$ and $b \mid n$.

- Examples: $\mathrm{lcm}(4, 9) = 36$, $\mathrm{lcm}(4, 10) = 20$.

- **Claim.** Let $a = \prod_1^n p_i^{\alpha_i}$ and $b = \prod_1^n p_i^{\beta_i}$ be the prime factorization of a, b. Then, $\mathrm{lcm}(a, b) = \prod_{i=1}^n p_i^{\max(\alpha_i, \beta_i)}$.

- **Proof.**
  - $\cdot$ $\exists \delta_i \in \mathbb{N}$ s.t. $\mathrm{lcm}(a, b) = \prod_{i=1}^n p_i^{\delta_i} \prod_{n+1}^N p_i^{\delta_i}$.
  - $\cdot$ $a \mid \mathrm{lcm}(a, b) \Rightarrow \delta_i \geq \alpha_i$ ($\alpha_{n+1} = \cdots = 0$).
  - $\cdot$ $b \mid \mathrm{lcm}(a, b) \Rightarrow \delta_i \geq \beta_i \Rightarrow \delta_i \geq \max(\alpha_i, \beta_i)$.
  - $\cdot$ Conversely, if $\exists 1 \leq i \leq N$ s.t $\delta_i > \max(\alpha_i, \beta_i)$ then $(\prod_1^n p_j^{\delta_j})/p_i$ would still be a multiple of a and of b contradicting the minimality of $\mathrm{lcm}(a, b)$.

- Example. $\mathrm{lcm}(95256, 432) =?$
  - $\cdot$ $432 = 2^4 3^2$, and $95256 = 2^3 3^5 7^2$
  - $\cdot$ $\Rightarrow \mathrm{lcm}(95256, 432) = 2^4 3^5 7^2 = 190512$.

- Do we really need to factor a and b?

lcm and gcd

- **Theorem.** Let $a, b \in \mathbb{N}^+$.

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

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

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta.$$

Congruence

- **Def.** Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}^+$. a is *congruent* to b modulo m if $m \mid a - b$: $\mathbf{a \equiv b \pmod{m}}$.
- Also, a "equals" b modulo m, and $a \not\equiv b \pmod{m}$.
- · Examples: $17 \equiv 5 \pmod{6}$
  · $24 \not\equiv 14 \pmod{6}$, but
  · $24 \equiv 14 \pmod{5}$
- **Claim.** For $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}^+$,

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

- **Proof.**

  · There exist $q_a, r_a, q_b, r_b \in \mathbb{Z}$ s.t.

$$\begin{aligned} a &= mq_a + r_a & \qquad 0 \le r_a < m \\ b &= mq_b + r_b & \qquad 0 \le r_b < m \end{aligned}$$

  · $\Rightarrow a - b = m(q_a - q_b) + (r_a - r_b)$

  · $\Rightarrow m \mid a - b \iff m \mid r_a - r_b$

  · Since $-m < r_a - r_b < m$

  · $m \mid a - b \iff r_a - r_b = 0.$

Congruence cont.

- **Corollary.** $a \equiv (a \bmod m) \pmod{m}$.
- **Proof.** $((a \bmod m) \bmod m) = (a \bmod m)$.
- **Claim.** Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}^+$.

$$a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z} : a = b + km.$$

- **Proof.**

$$a \equiv b \pmod{m} \iff m \mid a - b.$$

Congruence Classes

- **Def.** The *congruence class* of a modulo m is $\{b : b \equiv a \pmod{m}\}$.
- Example.
  - The congruence class of 1 modulo 2 is...
    the set of odd numbers.
  - The congruence class of 0 modulo 2 is the evens.
  - The two classes form a partition of $\mathbb{Z}$.
- More generally, for a fixed $m \in \mathbb{N}^+$ congruence modulo m is a relation on $\mathbb{Z}$ that is
  - reflexive: $a \equiv a \pmod{m}$
  - symmetric: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
  - transitive: $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$.
  - The latter follows from $a - c = (a - b) + (b - c)$.
- Thus, congruence mod m is an *equivalence relation.*
- An equivalence relation on S partitions S into equivalence classes.
- For the congruence relation these are the congruence classes.

Modular Arithmetics

- Arithmetics: $a = b$ and $c = d$ implies $a + c = b + d$.
- Do these manipulations hold for congruences?
- **Theorem.** Let $m \in \mathbb{N}^+$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$.
-
  - Example. $7 \equiv 2 \pmod{5}$, and $11 \equiv 1 \pmod{5}$
  - $\Rightarrow 18 \equiv 3 \pmod{5}$, and $77 \equiv 2 \pmod{5}$.
- **Proof.** $\exists k, l \in \mathbb{Z}$ s.t.
  - $a = b + km$, and $c = d + lm$
  - $\Rightarrow a + c = b + d + m(k + l)$
  - $\Rightarrow a + c \equiv b + d \pmod{m}$.
  - Similarly, $ac = bd + m(kd + bl + klm)$
  - $\Rightarrow ac \equiv bd \pmod{m}$.
- **Corollary.** For $m \in \mathbb{N}^+$, $a, b \in \mathbb{Z}$

$$ab \equiv (a \bmod m)(b \bmod m) \pmod{m}.$$

Modular Arithmetics cont.

- **Corollaries.** For $m, k \in \mathbb{N}^+$, $a, b \in \mathbb{Z}$
  - $(ab \bmod m) \equiv (a \bmod m)(b \bmod m) \pmod m$
  - $a^{2^k} \bmod m = \left(a^{2^{k-1}} \bmod m\right)^2 \bmod m$
- Efficient modular exponentiation: a^n, $a \in \mathbb{Z}, n \in \mathbb{N}$.
  - Let $n = (d_{p-1} \ldots d_1 d_0)_2$ (binary representation).

$$a^n = a^{\sum_{i=0}^{p-1} d_i 2^i} = \prod_{i=0}^{p-1} a^{d_i 2^i}.$$

  - Let

$$x_k := \Big(\prod_{i=0}^{k} a^{d_i 2^i}\Big) \bmod m = \left(x_{k-1} \cdot a^{d_k 2^k}\right) \bmod m$$

  - With $x_{-1} := 1$, for $k = 0 \ldots p-1$ compute

$$x_k = \left(x_{k-1} \cdot \begin{cases} a^{2^k} \bmod m & \text{if } d_k = 1 \\ 1 & \text{if } d_k = 0 \end{cases}\right) \bmod m,$$

and (for $k \geq 1$)

$$a^{2^k} \bmod m = \left(a^{2^{k-1}} \bmod m\right)^2 \bmod m.$$

Modular Arithmetics cont.

- For $a, b, c \in \mathbb{Z}$ with $c \neq 0$,

$$ac = bc \Rightarrow a = b.$$

- Does it carry over to the modular world?
- Example: $2 \cdot 4 \equiv 3 \cdot 4 \pmod{4}$ but $2 \not\equiv 3 \pmod{4}$.
- But $4 \equiv 0 \pmod{4}$!
- Example: $3 \cdot 2 \equiv 1 \cdot 2 \pmod{4}$ but $3 \not\equiv 1 \pmod{4}$.
- Shall we give up?
- **Theorem.** Let $m \in \mathbb{N}^+$ and $a, b, c \in \mathbb{Z}$. If $\gcd(c, m) = 1$ then $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$.
- **Proof.**

$$m \mid ac - bc \quad \Rightarrow \quad m \mid c(a - b) \quad \Rightarrow \quad m \mid (a - b).$$