Discrete Mathematics

(extended) Euclidean algorithm, prime number generation, linear congruence equation

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Euclidean Algorithm (EA)

ALGORITHM: compute $\gcd(a,b)$

- **Input**: $a, b\ (a \geq b > 0)$
- **Output**: $d = \gcd(a,b)$
  - $r_0 = a; r_1 = b;$
  - $r_0 = r_1 q_1 + r_2 \ \ (0 < r_2 < r_1)$
  - $\vdots$
  - $r_{i-1} = r_i q_i + r_{i+1} \ \ (0 < r_{i+1} < r_i)$
  - $\vdots$
  - $r_{k-2} = r_{k-1} q_{k-1} + r_k \ (0 < r_k < r_{k-1})$
  - $r_{k-1} = r_k q_k$
  - output r_k

$a = 12345, b = 123$		
i	r_i	q_i
0	12345	
1	123	100
2	45	2
3	33	1
4	12	2
5	9	1
6	3	3
7	0	

Correctness: $d = \gcd(r_0, r_1) = \cdots = \gcd(r_{k-1}, r_k) = r_k$

Extended Euclidean Algorithm (EEA)

ALGORITHM: compute $d = \gcd(a,b)$, s, t such that $as + bt = d$

- **Input**: a, b $(a \geq b > 0)$
- **Output**: $d = \gcd(a,b)$, integers s, t such that $d = as + bt$
  - $r_0 = a; r_1 = b;$ $\binom{s_0}{t_0} = \binom{1}{0}$; $\binom{s_1}{t_1} = \binom{0}{1}$;
  - $r_0 = r_1 q_1 + r_2$ $(0 < r_2 < r_1)$; $\binom{s_2}{t_2} = \binom{s_0}{t_0} - q_1 \binom{s_1}{t_1}$
  - $\vdots$
  - $r_{i-1} = r_i q_i + r_{i+1}$ $(0 < r_{i+1} < r_i)$; $\binom{s_{i+1}}{t_{i+1}} = \binom{s_{i-1}}{t_{i-1}} - q_i \binom{s_i}{t_i}$
  - $\vdots$
  - $r_{k-2} = r_{k-1} q_{k-1} + r_k$ $(0 < r_k < r_{k-1})$; $\binom{s_k}{t_k} = \binom{s_{k-2}}{t_{k-2}} - q_{k-1} \binom{s_{k-1}}{t_{k-1}}$
  - $r_{k-1} = r_k q_k$
  - output r_k, s_k, t_k

EEA

Correctness: We have that $r_i = as_i + bt_i$ for $i = 0,1,2, \ldots, k$

- $r_0 = a = (a,b)\binom{s_0}{t_0}$; $r_1 = b = (a,b)\binom{s_1}{t_1}$;
- $r_2 = r_0 - q_1 r_1 = (a,b)\binom{s_0}{t_0} - q_1 \cdot (a,b)\binom{s_1}{t_1} = (a,b)\binom{s_2}{t_2}$;
- $\vdots$
- $r_k = r_{k-2} - q_{k-1} r_{k-1} = (a,b)\binom{s_{k-2}}{t_{k-2}} - q_{k-1} \cdot (a,b)\binom{s_{k-1}}{t_{k-1}} = (a,b)\binom{s_k}{t_k}$

EXAMPLE: Execution of the EEA on input $a = 12345, b = 123$

i	r_i	q_i	s_i	t_i
0	12345		1	0
1	123	100	0	1
2	45	2	1	−100
3	33	1	−2	201
4	12	2	3	−301
5	9	1	−8	803
6	3	3	11	−1104
7	0			

Complexity

THEOREM: Let $\alpha = \frac{1}{2}(1+\sqrt{5})$. Then $k \leq \ln b / \ln \alpha + 1$ in EA.

- $k = 1$: $k \leq \ln b / \ln \alpha + 1$
- $k > 1$: we show that $r_{k-i} \geq \alpha^i$ for $i = 0,1,\dots,k-1$
  - $i = 0$: $r_k \geq 1 = \alpha^0$
  - $i = 1$: $r_{k-1} > r_k \Rightarrow r_{k-1} \geq r_k + 1 \geq 2 \geq \alpha^1$
  - Suppose that $r_{k-i} \geq \alpha^i$ for $i \leq j$
    - $$\begin{aligned} r_{k-(j+1)} &= r_{k-j} q_{k-j} + r_{k-(j-1)} \\ &\geq \alpha^j + \alpha^{j-1} \\ &= \alpha^{j-1}(\alpha + 1) \\ &= \alpha^{j+1} \end{aligned}$$
- $b = r_1 \geq \alpha^{k-1} \Rightarrow k \leq \ln b / \ln \alpha + 1$

Complexity of EA and EEA: $O(\ell(a)\ell(b))$ bit operations

Prime Number Theorem

DEFINITION: For $x \in \mathbb{R}^+$, $\pi(x) = \sum_{p \le x} 1$: # of primes $\le x$

THEOREM: $\lim\limits_{x\to\infty} \pi(x)/(x/\ln x) = 1$

- Conjectured by Legendre and Gauss
- Chebyshev: if the limit exists, then it is equal to 1
- Rosser and Schoenfeld:
  - $\pi(x) > \frac{x}{\ln x}(1 + \frac{1}{2\ln x})$ when $x \ge 59$
  - $\pi(x) < \frac{x}{\ln x}(1 + \frac{3}{2\ln x})$ when $x > 1$

NOTATION: $\mathbb{P}$- the set of all primes; $\mathbb{P}_n = \{p \in \mathbb{P}: 2^{n-1} \le p < 2^n\}$.

THEOREM: $|\mathbb{P}_n| \ge \frac{2^n}{n \ln 2}\left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right)$ when $n \to \infty$.

Number of n-bit Primes

EXAMPLE: The number of n-bit primes for $n \in \{10, \ldots, 25\}$.

n	$\lvert\mathbb{P}_n\rvert$	$2^{n-1}/n \ln 2$	n	$\lvert\mathbb{P}_n\rvert$	$2^{n-1}/n \ln 2$
10	75	73.8	18	10749	10505.4
11	137	134.3	19	20390	19904.9
12	255	246.2	20	38635	37819.4
13	464	454.6	21	73586	72036.9
14	872	844.2	22	140336	137525.0
15	1612	1575.8	23	268216	263091.4
16	3030	2954.6	24	513708	504258.5
17	5709	5561.7	25	985818	968176.3

Prime Number Generation

Basic Idea: randomly choose n-bit integers until a prime found.

- The number of n-bit integers is 2^{n-1}
- $|\mathbb{P}_n| \geq \frac{2^n}{n \ln 2}\left(\frac{1}{2} + O\left(\frac{1}{n}\right)\right)$ when $n \to \infty$
- The probability that a prime is chosen in every trial is equal to

$$\alpha_n = \frac{1}{n \ln 2}\left(1 + O\left(\frac{1}{n}\right)\right), n \to \infty$$

- In $\alpha_n^{-1} = \frac{n \ln 2}{1+O\left(\frac{1}{n}\right)} \leq 2n \ln 2$ trials, we get a prime.

Efficient Algorithms: An algorithm is considered as efficient if its (expected) running time is a polynomial in the bit length of its input. //a.k.a. (expected) polynomial-time algorithm

EXAMPLE: Choosing an n-bit prime can be done efficiently.

- The expected # of trials is $\leq 2n \ln 2$, a polynomial in n (input length)
- Determine if an n-bit integer is prime can be done efficiently

Linear Congruence Equations

DEFINITION: Let $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$. A **linear congruence equation** is a congruence of the form $ax \equiv b (\text{mod } n)$, where x is unknown.

THEOREM: Let $n \in \mathbb{Z}^+, a \in \mathbb{Z}$ and $d = \gcd(a, n)$. Then $ax \equiv b (\text{mod } n)$ has a solution if and only if $d|b$.

- $\Rightarrow$: suppose that $ax_0 \equiv b (\text{mod } n)$ for a specific $x_0 \in \mathbb{Z}$
  - $\exists z \in \mathbb{Z}$ such that $ax_0 - b = nz$
  - $b = ax_0 - nz$
  - $d|a, d|n \Rightarrow d|b$
- $\Leftarrow$: suppose that $d|b$ $\exists z \in \mathbb{Z}$ such that $b = dz$
  - $d = \gcd(a, n)$
    - $\exists s, t \in \mathbb{Z}$ such that $as + nt = d$
    - $b = dz = asz + ntz$
    - $a\,(sz) \equiv b\ (\text{mod } n)$
    - sz is a solution

Linear Congruence Equations

THEOREM: Let $n \in \mathbb{Z}^+, a \in \mathbb{Z}, \gcd(a, n) = d,\ t = \left(\frac{a}{d}\right)^{-1} \bmod \frac{n}{d}$.

If $d|b$, then $ax \equiv b \pmod{n}$ iff $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$.

- $t = \left(\frac{a}{d}\right)^{-1} \bmod \frac{n}{d}$ $\quad t \cdot \frac{a}{d} \equiv 1 \left(\bmod \frac{n}{d}\right)$ $\quad \exists s \in \mathbb{Z}$ such that $t \cdot \frac{a}{d} = 1 + s \cdot \frac{n}{d}$

- $ax \equiv b \pmod{n}$
- $\exists z \in \mathbb{Z}$ such that $ax - b = nz$
- $\frac{t}{d}(ax - b) = \frac{t}{d} nz$
- $\left(1 + s \cdot \frac{n}{d}\right) x - t\frac{b}{d} = t\frac{n}{d} z$
- $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$

- $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right)$
- $\exists z \in \mathbb{Z}$ such that $x - t\frac{b}{d} = \frac{n}{d} z$
- $ax - at\frac{b}{d} = a\frac{n}{d} z$
- $ax - \left(1 + s \cdot \frac{n}{d}\right) b = a \cdot \frac{n}{d} z$
- $ax \equiv b \pmod{n}$

System of Linear Congruences

Sun-Tsu's Question: There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

- $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$

DEFINITION: A **system of linear congruences** is a set of linear congruence equations of the form

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}.$$

- $x \in \mathbb{Z}$ is a **solution** if it satisfies all k equations.