School of Information Science and Technology
ShanghaiTech University

SI120 Discussion 1

Homework 1: Number Theory

SI120 TA Team

March 4, 2022

Review

What we have learned so far?

- Number theory: FTA and its application
- Equivalence relationship: congruence, $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$.
- The cardinality of $\mathbb{Z}_n^*$:$\phi(n)$
- Ideal and greatest common divisor.
- Euler Theorem and Fermat's Little Theorem.

Review

What we have learned so far?

- Information security: Confidentiality
- Public-key cryptosystem: RSA
- The security of RSA
  - Factoring problem.
  - $O(\sqrt{N})$, polynomial?
- Implementation of RSA:
  - Primality test.
  - Square and multiply.
  - Extended Euclidean Algorithm

Exercise

Let $a, b \in \mathbb{Z}$ and $a \neq 0$. Which of the following statement is correct?

A. a divides b if there is an integer $c \in \mathbb{Z}$ such that $a = bc$.

B. $n \in \mathbb{Z}^+$ is not a prime, then n is called a composite.

C. The set $\mathbb{Z}^*_{1999}$ has 1998 elements.

D. According to FTA, every integer $n \geqslant 1$ cound be uniquely written as $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, ..., p_r$ are distinct primes and $e_1, ..., e_r \geq 1$.

Exercise

Which of the following statement is correct?

A. If a, b are integers, then there exists integers q, r such that $a = bq + r$ and $0 < r < b$, where $q = \lfloor \frac{a}{b} \rfloor$.

B. $\lfloor \lfloor x \rfloor + 0.5 \rfloor = \lfloor x + 0.5 \rfloor$ for all real number x.

C. If I_1 and I_2 are ideals of $\mathbb{Z}$, then $I_1 + I_2$ is also an ideal of $\mathbb{Z}$.

D. Suppose p is a prime and $p|ab$, then $p|a$ and $p|b$.

Exercise

Which of the following is not equivalence relation?

A. $S = \{(x, y) : x, y \in \mathbb{R}, x \equiv y \mod 1997\}$ on $\mathbb{R}$.

B. $S = \{(x, y) : x, y \in \mathbb{R}, x - y \in \mathbb{Z}\}$ on $\mathbb{R}$.

C. $S = \{(x, y) : x, y \in \mathbb{R}, x + y \in \mathbb{Z}\}$ on $\mathbb{R}$.

D. $S = \{(x, y) : x, y \in \mathbb{R}, x - y \in \mathbb{Q}\}$ on $\mathbb{R}$.

Exercise

Which of the following is equivalent to $\mathbb{Z}_8^*$?

A. $\{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$

B. $\{[0]_8, [1]_8, [3]_8, [5]_8, [7]_8\}$

C. $\{[-1]_8, [3]_8, [5]_8, [-7]_8\}$

D. $\{[-1]_8, [-3]_8, [-5]_8, [-6]_8, [-7]_8\}$

Exercise

Let $\phi(n)$ be the Euler's Phi function, and $n = 5^3 \times 7 \times 13^2$. Then $\phi(n) =$

A. 93400.

B. 93500.

C. 93600.

D. 93700.

Which of the following statement is correct?

A. Let p and q be any two primes and $n = pq$, then $\phi(n) = (p-1)(q-1)$.

B. According to the Euler's Theorem, if $n \geq 1$ and $\alpha \in \mathbb{Z}_n$, then $\alpha^{\phi(n)} \equiv 1(\text{mod } n)$.

C. If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, ..., p_k$ and integers $e_1, ..., e_k \geq 1$, then $\phi(n) = n(1-p_1) \cdots (1-p_k)$.

D. According to Fermat's Little Theorem, if p is a prime and $\alpha \in \mathbb{Z}_p$, then $\alpha^p \equiv \alpha(\text{mod } p)$.

Which of the following statements about RSA cryptosystem is correct?

A. The two primes p and q are computed by deterministic algorithm.

B. Given $N = pq$, we can factor it in $O(\sqrt{N})$ time, which is polynomial, so we can factor it efficiently.

C. Choosing a small d in public key would speed up the encryption.

D. We can compute $a^e (\bmod n)$ in $O\left(\ell(e)\ell(n)^2\right)$ time.

Homework 1

Question 1

Show that $\log_5 7$ is an irrational number.

Idea

By contradiction!

Question 1

Show that $\log_5 7$ is an irrational number.

Solution: By contradiction.

- If $\log_5 7$ is rational, then $\exists p, q \in \mathbb{Z}^+ \ \gcd(p, q) = 1$ such that $\log_5 7 = \frac{q}{p}$.
- $5^q = 7^p$, impossible. Why?
  - By the uniqueness of FTA.
  - RHS will never be a multiple of 5, or the LHS will never be a multiple of 7.
    - Show by enumeration, infeasible when the numbers are large.
    - **Theorem:** If n is a prime, then the product of two non-zero elements in $\mathbb{Z}_n$ is non-zero.
    - 5 is called a generator of $\mathbb{Z}_7^*$ and vice versa.

Homework1

Question 2

Let p be a prime and k be a integer such that $0 < k < p$. Show that $\binom{p}{k}$ is a multiple of p.

Ideas

- Show that $p|\binom{p}{k}$.
- Show that $\frac{(p-1)!}{k!(p-k)!}$ is also a integer.
- $\ldots$

Homework1

Question 2

Let p be a prime and k be a integer such that $0 < k < p$. Show that $\binom{p}{k}$ is a multiple of p.

Solution 1

- $\binom{p}{k} = \frac{p(p-1)!}{k(k-1)![(p-1)-(k-1)]!} = \frac{p}{k}\binom{p-1}{k-1}$
- $k\binom{p}{k} = p\binom{p-1}{k-1} \quad \Rightarrow \quad p|k\binom{p}{k}$
- $p \nmid k \quad \Rightarrow \quad p|\binom{p}{k}$

Homework1

Question 2

Let p be a prime and k be a integer such that $0 < k < p$. Show that $\binom{p}{k}$ is a multiple of p.

Solution 2

- $p|p!$, $p! = \binom{p}{k}k!(p-k)!$
- $p|\binom{p}{k}k!(p-k)!$
- $p|\binom{p}{k}$
  - $\gcd(p, k!) = \gcd(p, (p-k)!) = 1$

Question 2

Let p be a prime and k be a integer such that $0 < k < p$. Show that $\binom{p}{k}$ is a multiple of p.

Solution 3

- $\binom{p}{k}$ is an integer, so $k!(p-k)!|p!$
- $k!(p-k)!|p(p-1)!$
- p is a prime, so $k!(p-k)!|(p-1)!$
- $\frac{(p-1)!}{k!(p-k)!}$ is also an integer.

Question 2

Let p be a prime and k be a integer such that $0 < k < p$. Show that $\binom{p}{k}$ is a multiple of p.

Solution 4

- p is the largest prime factor of $\binom{p}{k}$
- $\binom{p}{k} = \prod_{i=1}^{n} p_i^{e_i} \cdot p$
- So $\frac{(p-1)!}{k!(p-k)!} = \prod_{i=1}^{n} p_i^{e_i}$ is also an integer.

Question 3

Let $a, b > 1$ be relatively prime integers. Show that if $a|n$ and $b|n$, then $ab|n$.

Solution 1:

- $a|n \Rightarrow \exists k_1 \in \mathbb{N} \quad n = k_1 a$
- $b|n \Rightarrow b|k_1 a \xrightarrow{gcd(b,a)=1} b|k_1$
- $b|k_1 \Rightarrow \exists k_2 \in \mathbb{N} \quad k_1 = k_2 b$
- $n = k_1 a = k_2 ab \Rightarrow ab|n$

Question 3

Let $a, b > 1$ be relatively prime integers. Show that if $a|n$ and $b|n$, then $ab|n$.

Solution 2: Bézout's Identity

- There exist integers s, t such that $gcd(a, b) = as + bt = 1$
- $b|n \Rightarrow ba|na \Rightarrow ba|nas$
  $a|n \Rightarrow ab|nb \Rightarrow ab|nbt$
- $ab|nas + nbt \Rightarrow ab|n$

Homework 1

Question 3

Let $a, b > 1$ be relatively prime integers. Show that if $a|n$ and $b|n$, then $ab|n$.

Solution 3:Fundamental Theorem of Arithmetic

- $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, p_1 < p_2 < \cdots p_k, p_1 < p_2 < \cdots < p_k$ are distinct primes and $\forall i, n_i \geqslant 1$
- $a|n, b|n \Rightarrow a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $\forall k, a_k \leqslant n_k, b_k \leqslant n_k$
- $ab = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}$
- $gcd(a, b) = 1 \Rightarrow \forall k, a_k \times b_k = 0$
  $a_k + b_k = max\{a_k, b_k\} \leqslant n_k$
- $ab|n$

Homework 1

Question 4

Let $a, b, c \in \mathbb{Z}^+$. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$.

Solution 1: B*é*zout's Identity

Sufficiency:

- $\gcd(a, bc) = 1$, then $\exists s, t \in \mathbb{Z}$ such that $as + bct = 1$.
- $as + b(ct) = 1$, then $\gcd(a, b) = 1$.
- $as + c(bt) = 1$, then $\gcd(a, c) = 1$.

Necessity:

- $\gcd(a, b) = 1$, then $as_1 + bt_1 = 1$.
- $\gcd(a, c) = 1$, then $as_2 + ct_2 = 1$.
- $(1 - as_1)(1 - as_2) = bct_1 t_2$.
- $a(s_1 + s_2 - as_1 s_2) + bc(t_1 t_2) = 1$, then $\gcd(a, bc) = 1$.

Question 4

Let $a, b, c \in \mathbb{Z}^+$. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$.

Solution 2: Proof by contradiction

Sufficiency:

- Suppose $\gcd(a, b) = m > 1$, WLOG.
- $m|a, m|b \Rightarrow m|bc$.
- $\gcd(a, bc) \geq m > 1$, contradict.

Question 4

Let $a, b, c \in \mathbb{Z}^+$. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$.

Solution 3: Proof by FTA

By FTA, we have $a = \prod_{i=1}^n p_i^{\alpha_i}$,$b = \prod_{i=1}^n p_i^{\beta_i}$,$c = \prod_{i=1}^n p_i^{\gamma_i}$ where $\alpha_i, \beta_i, \gamma_i \geq 0$, so $bc = \prod_{i=1}^n p_i^{\beta_i+\gamma_i}$.

Sufficiency:

- $\gcd(a, bc) = \prod_{i=1}^n p_i^{\min(\alpha_i, \beta_i+\gamma_i)} = 1$.
- $\beta_i + \gamma_i \geq \beta_i \Rightarrow \min(\alpha_i, \beta_i + \gamma_i) \geq \min(\alpha_i, \beta_i)$
- $\gcd(a, b) = \prod_{i=1}^n p_i^{\min(\alpha_i, \beta_i)} = 1$

Homework 1

Question 4

Let $a, b, c \in \mathbb{Z}^+$. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = \gcd(a, c) = 1$.

Solution 3: Proof by FTA

By FTA, we have $a = \prod_{i=1}^{n} p_i^{\alpha_i}, b = \prod_{i=1}^{n} p_i^{\beta_i}, c = \prod_{i=1}^{n} p_i^{\gamma_i}$ where $\alpha_i, \beta_i, \gamma_i \geq 0$, so $bc = \prod_{i=1}^{n} p_i^{\beta_i+\gamma_i}$.

Necessity:

- $\gcd(a, b) = \gcd(a, c) = 1 \Rightarrow \alpha_i\beta_i = 0, \alpha_i\gamma_i = 0$
- $\alpha_i(\beta_i + \gamma_i) = 0$
- $\min(\alpha_i, \beta_i + \gamma_i) = 0$
- $\gcd(a, bc) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i+\gamma_i)} = 1$

Homework 1

Question 5

Let $S = (\mathbb{R} \times \mathbb{R}) \backslash \{(0,0)\}$. Let $R = \{((a,b),(c,d)) : (a,b),(c,d) \in S$ and $\exists \lambda \in \mathbb{R} \backslash \{0\}$ such that $(a,b) = (\lambda c, \lambda d)\}$. Show that R is an equivalence relation.

Solution: by definition

- **Reflexive:** $\lambda = 1$
- **Symmetric:** $\lambda' = \frac{1}{\lambda}$
- **Transitive** $\lambda' = \lambda_1 \lambda_2$

That’s all today.
Have a nice weekend.