上 海 交 通 大 学 试 卷

2021 – 2022 Academic Year (Fall Term)

Ve203 Discrete Mathematics
Second Midterm Exam

Exercise 1 (20 points)

(i)	(ii)	(iii)	(iv)	(v)
BCD	A	AD	BCD	ACD

(i) Let $m, n \in \mathbb{N} \setminus \{0\}$, and φ be the Euler totient function, which of the following is correct?

A. $\varphi(2m) = 2\varphi(m)$ if m is prime.

B. If $n \geq 3$, then $\varphi(n)$ is even.

C. If $m \mid n$, then $(\mathbb{Z}/n\mathbb{Z})^\times$ admits a subgroup of order $\varphi(m)$.

D. If $m \mid n$, then $\varphi(mn) = m\varphi(n)$.

(ii) Given finite group G and subgroups $H, K \leq G$. Which of the following is correct?

A. If G is cyclic, then $H \trianglelefteq G$, i.e., H is a normal subgroup of G.

B. If H is abelian, then $H \trianglelefteq G$.

C. $|H \cap K| = \operatorname{lcm}(|H|, |K|)$.

D. If $xy = yx$ for all $x, y \in H$, then $H \trianglelefteq G$.

(iii) Given finite group G, subgroup $H \leq G$, $x, y \in G$. Which of the following is correct?

A. $|xH| = |Hx|$.

B. either $xH = Hy$ or $xH \cap Hy = \varnothing$.

C. $xH = yH$ if $xy \in H$.

D. $[G : H] = |G|/|H|$.

(iv) Given group G and G', and homomorphism $f : G \to G'$, which of the following statement is correct?

A. If $x \in G$, then $|f(x)|$ divides $|x|$.

B. If G is cyclic, then $f(G)$ is also cyclic.

C. If G is abelian, then $f(G)$ is also abelian.

D. If $G = G'$ and $f(x) = x^{-1}$, then G is abelian.

(v) Given $a_1, \ldots, a_n \in \mathbb{N} \setminus \{0\}$, which of the following statement is correct?

A. If $a_1, \ldots, a_n$ are pairwise coprime, then $\gcd(a_1, \ldots, a_n) = 1$.

B. If $\gcd(a_1, \ldots, a_n) = 1$, then $a_1, \ldots, a_n$ are pairwise coprime.

C. If $a_1, \ldots, a_n$ are pairwise coprime, then $\operatorname{lcm}(a_1, \ldots, a_n) = a_1 a_2 \ldots a_n$.

D. If $\operatorname{lcm}(a_1, \ldots, a_n) = a_1 a_2 \ldots a_n$, then $a_1, \ldots, a_n$ are pairwise coprime.

Exercise 2 (10 points)

Given $a, n \in \mathbb{N}$ and $a, n > 1$, show that $n \mid \varphi(a^n - 1)$.

Solution: Let $m = 2^n - 1$, consider the multiplicative group $G = (\mathbb{Z}/m\mathbb{Z})^\times$, note that $a \in G$ since $\gcd(a, m) = \gcd(a, a^n - 1) = 1$. Next we show that the order of a is n. Indeed, since $m = a^n - 1$, thus $m \mid a^n - 1$, i.e., $a^n \equiv 1 \pmod m$. Also $a^x \not\equiv 1 \pmod m$ for $1 < x < m$ since $1 < a^x < a^n = m$. Thus the order of a is n. According to Lagrange's theorem, therefore the order of a divides the order of G, that is, $n \mid \varphi(2^n - 1)$. □

Exercise 3 (10 points)
Given group G and $a \in G$ a fixed element, define $\gamma_a : G \to G$, by $\gamma_a(x) = axa^{-1}$.

(i) (5 points) Show that γ_a is an isomorphism.

Solution:

- γ_a is a homomorphism. Indeed, since for all $x, y \in G$,
$$\gamma_a(x)\gamma_a(y) = (axa^{-1})(aya^{-1}) = axya^{-1} = \gamma_a(xy)$$
- γ_a is injective. Indeed, if $\gamma_a(x) = 1_G$, i.e., $axa^{-1} = 1_G$, we have $x = a \cdot 1_G \cdot a^{-1} = 1_G$. Hence γ_a is injective.
- γ_a is surjective. Indeed, given $y \in G$, we can find $x = a^{-1}ya \in G$ such that $\gamma_a(x) = a(a^{-1}ya)a^{-1} = y$.

Therefore γ_a is an isomorphism. □

Note that bijectiveness also follows from (ii), since

$$\gamma_g \circ \gamma_{g^{-1}} = \gamma_{1_G} = \gamma_{g^{-1}} \circ \gamma_g \tag{1}$$

(ii) (5 points) If $a, b \in G$, show that $\gamma_a \circ \gamma_b = \gamma_{ab}$.

Solution: Let $x \in G$, then

$$(\gamma_a \circ \gamma_b)(x) = \gamma_a(\gamma_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \gamma_{ab}(x) \tag{2}$$

Since x is arbitrary, thus statement follows. □

Exercise 4 (10 points)
Given that the Euler totient function φ is multiplicative, use this fact to show that the divisor sum formula holds, i.e.

$$n = \sum_{d \mid n} \varphi(d)$$

(You may also use the fact that $\varphi(1) = 1$ and $\varphi(p^k) = p^k - p^{k-1}$ for $p \in \mathbb{P}$, $k \in \mathbb{N} \setminus \{0\}$)

Solution 1: Proof by (strong) induction on n.

Base case: $n = 1$. Immediate since $\varphi(1) = 1$.

Inductive case: $n > 1$. Assume that the formula holds for positive integers less than n. Now write $n = mp^k$ where $\gcd(m, p) = 1$, p prime, and $k \geq 1$, (this can always be achieved by fundamental theorem of arithmetic), the divisors of n are thus given by dp^i, where $d \mid m$ and $0 \leq i \leq k$. Therefore

$$\sum_{d|n} \varphi(d) = \sum_{i=1}^{k} \sum_{d|m} \varphi(dp^i) = \sum_{i=1}^{k} \varphi(p^i) \sum_{d|m} \varphi(d) \tag{3}$$

$$= m \sum_{i=1}^{k} \varphi(p^i) = m \left[1 + \sum_{i=1}^{k} (p^i - p^{i-1}) \right] \tag{4}$$

$$= mp^k = n. \tag{5}$$

Therefore the divisor sum formula holds. $\square$

Solution 2: By fundamental theorem of arithmetic, we can write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$. First note that

$$\sum_{e_j=1}^{\alpha_j} \varphi(p_j^{e_j}) = \varphi(1) + \varphi(p_j) + \cdots + \varphi(p_j^{\alpha_j}) \tag{6}$$

$$= 1 + \sum_{e_j=1}^{\alpha_j} (p_j^{e^j} - p_j^{e_j-1}) = p_j^{\alpha_j} \tag{7}$$

Since powers of distinct primes are coprime, thus

$$\sum_{d|n} \varphi(d) = \sum_{e_1=0}^{\alpha_1} \cdots \sum_{e_r=0}^{\alpha_r} \varphi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \tag{8}$$

$$= \left[\sum_{e_1=0}^{\alpha_1} \varphi(p_1^{e_1}) \right] \cdots \left[\sum_{e_r=0}^{\alpha_r} \varphi(p_r^{e_r}) \right] \tag{9}$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = n \tag{10}$$

which is the divisor sum formula. $\square$

Exercise 5 (20 points)

(i) (10 points) Let $G = \langle a \rangle$ be of order rs, where $\gcd(r, s) = 1$. Show that there are unique $b, c \in G$ with $|b| = r$ and $|c| = s$ such that $a = bc$.

Solution:

Existence: Since $\gcd(r,s)=1$, then there exsits $m,n\in\mathbb{Z}$ such that $rm+sn=1$. If we let $b=a^{sn}\in G$ and $c=a^{rm}\in G$, then we have

$$bc = a^{sn}a^{rm} = a^{rm+sn} = a^1 = a \tag{11}$$

Sicne $b=a^{sn}$, then order of b is given by

$$|b| = \frac{rs}{\gcd(sn,rs)} = \frac{rs}{s\cdot\gcd(r,n)} = \frac{rs}{s\cdot 1} = r \tag{12}$$

where $\gcd(r,n)=1$ since $rm+sn=1$. Similarly $|c|=s$.

Uniqueness: Suppose that $a=bc=b'c'$, where $|b|=|b'|=r$, and $|c|=|c'|=s$. Since G is cyclic, thus $\langle a\rangle=\langle a'\rangle$ and $\langle b\rangle=\langle b'\rangle$. Let $c'=c^y$, $y\in\mathbb{Z}$, thus $a=bc=b'c^y$. Therefore $a^r=b^rc^r=(b')^rc^{ry}$. Since $|b|=|b'|=r$, we have $c^r=c^{ry}$. But note that $|c^r|=s$ (since $\gcd(r,s)=1$), thus $y\equiv 1 \pmod{s}$, so $c^y=c$, i.e., $c'=c$. Similarly $b=b'$. □

(Uniqueness. If $a=bc=b'c'$, then $b^{-1}b'=(c')^{-1}c\in\langle b\rangle\cap\langle c\rangle$. But since $\gcd(|b|,|c|)=1$, we have $\langle b\rangle\cap\langle c\rangle=\{1_G\}$ (otherwise $|b|$ should divide $|\langle c\rangle|$ etc.) Therefore $b=b'$ and $c=c'$.)

(ii) (10 points) Use part (i) to show that if $\gcd(r,s)=1$, then $\varphi(rs)=\varphi(r)\varphi(s)$.

Solution: Since $G=\langle a\rangle$ and $|G|=rs$, thus the number of generators in G is given by $\varphi(rs)$. On the other hand, we know from part (i) that there is a one-to-one correspondence between the generator $a\in G$ and a pair $(b,c)\in G\times G$, with $|b|=r$ and $|c|=s$. Therefore number of generators for $\langle b\rangle$ and $\langle c\rangle$ are given by $\varphi(r)$ and $\varphi(s)$, respectively. Now there are $\varphi(r)\varphi(s)$ ways to form the generator $a=bc\in G$. Hence the identity holds. □

Exercise 6 (10 points)
Solve the following system of linear Diophantine equations,

$$x\equiv 3 \pmod{8},\qquad x\equiv 1 \pmod{15},\qquad x\equiv 11 \pmod{20}$$

Solution: Note that by Chinese remainder's theorem, the original system is equivalent to

$$x\equiv 3 \pmod{8} \tag{13}$$
$$x\equiv 1 \pmod{3} \tag{14}$$
$$x\equiv 1 \pmod{5} \tag{15}$$
$$x\equiv 11 \pmod{4} \tag{16}$$
$$x\equiv 11 \pmod{5} \tag{17}$$

Note that (13) implies (16), and (15) and (17) are the same, hence the original system is equivalent to

$$x \equiv 3 \pmod 8 \tag{18}$$
$$x \equiv 1 \pmod 5 \tag{19}$$
$$x \equiv 1 \pmod 3 \tag{20}$$

where the moduli are pairwise coprime. Note that (19) and (20) implies that $x \equiv 1 \pmod{15}$, we therefore can reduced the system above into

$$x \equiv 3 \pmod 8 \tag{21}$$
$$x \equiv 1 \pmod{15} \tag{22}$$

Let $x = 15y + 1 = 8z + 3$, thus $15y - 8z = 2$. By inspection, we have $(15)(1) - (8)(2) = -1$, thus we can choose $y = -2$ and $z = -4$ such that $15y - 8z = 2$. Now $x = 15y + 1 = -29$. Therefore the solution to the original system of Diophantine equation is given by

$$x \equiv -29 \pmod{120} \tag{23}$$

Exercise 7 (20 points)
In an RSA procedure, the public key is chosen as $(n, E) = (2077, 97)$, i.e., the encryption function e is given by

$$e(x) = x^{97} \pmod{2077}$$

(Note that $2077 = 31 \times 67$.)

(i) (10 points) Compute the private key D, where $D = E^{-1} \pmod{\varphi(n)}$. Show your work.

Solution: Note that $\varphi(2077) = (31 - 1)(67 - 1) = 1980$. We need to solve $97D \equiv 1 \pmod{1980}$. By Euclidean algorithm (or anything else that works)

$$1980 = 97 \times 20 + 40 \tag{24}$$
$$97 = 40 \times 2 + 17 \tag{25}$$
$$40 = 17 \times 2 + 6 \tag{26}$$
$$17 = 6 \times 2 + 5 \tag{27}$$
$$6 = 5 \times 1 + 1 \tag{28}$$

hence

$$\begin{aligned}
1 &= 6 - 5 && (29)\\
&= 6 - (17 - 6 \times 2) = 6 \times 3 - 17 && (30)\\
&= (40 - 17 \times 2) \times 3 - 17 = 40 \times 3 - 17 \times 7 && (31)\\
&= 40 \times 3 - (97 - 40 \times 2) \times 7 = 40 \times 17 - 97 \times 7 && (32)\\
&= (1980 - 97 \times 20) \times 17 - 97 \times 7 && (33)\\
&= 1980 \times 17 - 97 \times 347 && (34)
\end{aligned}$$

Thus $D \equiv -347 \equiv 1633 \pmod{1980}$.

(ii) (10 points) Decrypt the message 279, that is, find x if $y = e(x) = 279 \pmod{2077}$. Show your work.

Solution: We need to calculate $279^D \pmod{2077}$. First note that

$$1633 = (11001100001)_2 = 2^{10} + 2^9 + 2^6 + 2^5 + 2^0 \tag{35}$$

Then

$$
\begin{aligned}
279^{2^0} &\equiv 279 \pmod{2077} && (36)\\
279^{2^1} &\equiv 279^2 \equiv 992 \pmod{2077} && (37)\\
279^{2^2} &\equiv 992^2 \equiv -434 \pmod{2077} && (38)\\
279^{2^3} &\equiv (-434)^2 \equiv -651 \pmod{2077} && (39)\\
279^{2^4} &\equiv (1426)^2 \equiv 93 \pmod{2077} && (40)\\
279^{2^5} &\equiv 93^2 \equiv 341 \pmod{2077} && (41)\\
279^{2^6} &\equiv 341^2 \equiv (-31) \pmod{2077} && (42)\\
279^{2^7} &\equiv (-31)^2 \equiv 961 \pmod{2077} && (43)\\
279^{2^8} &\equiv 961^2 \equiv 1333 \pmod{2077} && (44)\\
279^{2^9} &\equiv 1333^2 \equiv 1054 \pmod{2077} && (45)\\
279^{2^{10}} &\equiv 1054^2 \equiv -279 \pmod{2077} && (46)
\end{aligned}
$$

Hence

$$
\begin{aligned}
279^{1871} &\equiv 279^{2^0+2^5+2^6+2^9+2^{10}} && (47)\\
&\equiv 279^{2^0} \cdot 279^{2^5} \cdot 279^{2^6} \cdot 279^{2^9} \cdot 279^{2^{10}} && (48)\\
&\equiv (279)(341)(-31)(1054)(-279) && (49)\\
&\equiv (-403)(-31)(1054)(-279) && (50)\\
&\equiv (31)(1054)(-279) && (51)\\
&\equiv (-558)(-279) && (52)\\
&\equiv 1984 \pmod{2077} && (53)
\end{aligned}
$$