CS201 · Discrete Mathematics

Assignment 3

刘乐奇 / 12011327

April 6, 2022

1 Q1

By definition, since $a|b$, we have $\exists c \in \mathbb{Z}, b = ca$. Similarly, we have $\exists d \in \mathbb{Z}, a = db$. So $b = ca = cdb \implies (cd-1)b = 0$.
For $b = 0$, it is clear that $a = 0$ such that $a = b$ or $a = -b$ is satisfied.
For $b \neq 0$, we have $cd = 1$, which has a solution of $c = 1, d = 1$ or $c = -1, d = -1$. Therefore, $a = b$ or $a = -b$. ■

2 Q2

1. Since $1768 = 16 \times 110 + 8, 110 = 16 \times 6 + 14, 6 = 16 \times 0 + 6$, then $(1768)_{10} = (6E8)_{16}$.
2. Since $010_2 = 2_8, 101_2 = 5_8$, then $(10101)_2 = (25)_8$.
3. Since $3_{16} = 0011_2, B_{16} = 1011_2, 5_{16} = 0101_2, A_{16} = 1010_2$, then $(3B5A)_{16} = (11101101011010)_2$.

3 Q3

1. $256 = 2^8$
2. $1890 = 2 \times 3^3 \times 5 \times 7$
3. $5! = 2^3 \times 3 \times 5$

4 Q4

1. By Euclidean algorithm,

$$\begin{aligned}
267 &= 3 \times 79 + 30 \\
79 &= 2 \times 30 + 19 \\
30 &= 1 \times 19 + 11 \\
19 &= 1 \times 11 + 8 \\
11 &= 1 \times 8 + 3 \\
8 &= 2 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\
2 &= 2 \times 1
\end{aligned}$$

   we can get $\gcd(267, 79) = 1$

2. From Euclidean algorithm, we have $q_1 = 3, q_2 = 2, q_3 = q_4 = q_5 = 1, q_6 = 2, q_7 = 1, q_8 = 2$. By extended Euclidean algorithm, from $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$, and for $j = 2, 3, 4, 5, 6, 7, 8$, we have

$$s_j = s_{j-2} - q_{j-1}s_{j-1},\ t_j = t_{j-2} - q_{j-1}t_{j-1}$$

   Finally, we can get $s_8 = 29, t_8 = -98$. Thus, $1 = \gcd(267, 79) = 267 \times 29 + 79 \times (-98)$

5 Q5

In this problem, we need to use a lemma: if $d|a$ and $d|b$, then $d|gcd(a,b)$. Here is the proof:
By Bezout's theorem, $gcd(a,b) = sa + tb$ for some integer s and t. Since $d|a$ and $d|b$, s and t are integers, by the property of division, then we have $d|sa + tb = gcd(a,b)$. ■
Then we can start the proof as requested in the problem.
Let $p = gcd(gcd(a,b),y)$, $q = gcd(d_1,d_2)$ and $r = gcd(a,b)$.
By the definition of greatest common divisor, we have

$$\begin{aligned} p|gcd(a,b),\ i.e.,\ p|r, &\qquad p|y \\ r|a, &\qquad r|b \end{aligned}$$

By the property of division, we have

$$p|a, \qquad p|b, \qquad p|y$$

By the lemma we had introduced, we have

$$\begin{aligned} p|gcd(a,y) = d_1\ (since\ p|a\ and\ p|y) \\ p|gcd(b,y) = d_2\ (since\ p|b\ and\ p|y) \end{aligned}$$

Thus (also the lemma),

$$p|gcd(d_1,d_2) = q \tag{1}$$

Conversely, since $q = gcd(d_1,d_2)$, by the definition of greatest common divisor, we have

$$\begin{aligned} q|d_1 = gcd(a,y) \\ q|d_2 = gcd(b,y) \end{aligned}$$

Since

$$\begin{aligned} gcd(a,y)|a, &\qquad gcd(a,y)|y \\ gcd(b,y)|b, &\qquad gcd(b,y)|y \end{aligned}$$

by the property of division, we have

$$q|a, \qquad q|b, \qquad q|y$$

By the lemma we had introduced, we have

$$q|gcd(a,b)\ (since\ q|a\ and\ q|b)$$

Thus (also the lemma),

$$q|gcd(gcd(a,b),y) = p \tag{2}$$

By expression (1) and (2), we ahve

$$p|q, \qquad q|p$$

As proved in Q1, we have $p = q$ or $p = -q$. Since p and q are positive integers, we have $p = q$, i.e.,

$$gcd(gcd(a,b),y) = gcd(d_1,d_2)$$

■

6 Q6

Let $c = gcd(a+b, a-b)$, then by definition we have

$$c|(b+a) \implies \exists m \in \mathbb{Z}, b+a = cm$$
$$c|(b-a) \implies \exists n \in \mathbb{Z}, b-a = cn$$

So we can get

$$2a = (m-n)c,\ 2b = (m+n)c$$

i.e., $c|2a, c|2b$.
Suppose $gcd(a,c) = k$ and $gac(b,c) = l$. Since

$$b - a = cn,\ i.e.,\ b = cn + a$$

we have $gcd(b,c) = gcd(a,c)$ by the lemma of Euclidean algorithm. Thus, we have $k|a$ and $l = k|b$, i.e., k is a common divisor of a and b.
Since $0 < k \leq gcd(a,b) = 1$ and $k \in \mathbb{Z}$, we have $k = 1$. Thus, $gcd(a,c) = gac(b,c) = 1$. Then we have

$$c|2$$

since $gcd(a,c) = gac(b,c) = 1$ and $c|2a, c|2b$.
Therefore, $\exists q \in \mathbb{Z}^+$,

$$2 = cq \geq c = gcd(b+a, b-a)$$

■

7 Q7

1. Take $p = 4$ (not a prime) and $a = 2$ (not divisible by p). We have $a^{p-1} = 2^3 \not\equiv 1(mod\ p) = 1(mod\ 4)$ since $2^3 \mod 4 = 0$ but $1 \mod 4 = 1$.

2.
   - By Fermat's little theorem, we have $302^{10} \equiv 1(mod\ 11)$ since 11 is a prime and 302 cannot be divided by 11. So

     $$302^{302} = 302^{30\times10+2} = (302^{10})^{30} \times 302^2 \equiv 302^2(mod\ 11)$$

     Since $302^2 = (11 \times 27 + 5)^2 \equiv 5^2 \equiv 3(mod\ 11)$, we have $302^{302} \mod 11 = 3$.

   - By Fermat's little theorem, we have $4762^{12} \equiv 1(mod\ 13)$ since 13 is a prime and 4762 cannot be divided by 13. So

     $$4762^{5367} = 4762^{447\times12+3} = (4762^{12})^{447} \times 4762^3 \equiv 4762^3(mod\ 13)$$

     Since $4762^3 = (13 \times 366 + 4)^3 \equiv 4^3 = 12(mod\ 13)$, we have $4762^{5367} \mod 13 = 4762^3 = 12$.

   - By Fermat's little theorem, we have $4^{522} \equiv 1(mod\ 523)$ since 523 is a prime and 4 cannot be divided by 523. So

     $$2^{39674} = 4^{83\times239} = 4^{38\times522+1} = (4^{522})^{38} \times 4 \equiv 4(mod\ 523)$$

     that is, $2^{39674} \mod 523 = 4$.

8 Q8

1. By Euclidean algorithm,

$$\begin{aligned}267 &= 3\times 79+30\\ 79 &= 2\times 30+19\\ 30 &= 1\times 19+11\\ 19 &= 1\times 11+8\\ 11 &= 1\times 8+3\\ 8 &= 2\times 3+2\\ 3 &= 1\times 2+1\\ 2 &= 2\times 1\end{aligned}$$

   we can get $\gcd(267,79)=1$. By extended Euclidean algorithm, from $s_0=1, s_1=0, t_0=0, t_1=1$, and for $j=2,3,4,5,6,7,8$, we have

$$s_j = s_{j-2} - q_{j-1}s_{j-1},\ t_j = t_{j-2} - q_{j-1}t_{j-1}$$

   Finally, we can get $s_8=29, t_8=-98$. Thus, $1=\gcd(267,79)=267\times 29+79\times(-98)$. So 29 is the inverse of $267 mod 79$. Therefore, $29\times 267x \equiv 29\times 3(mod\ 79) \implies x\equiv 87(mod\ 79)$.

2. By Euclidean algorithm,

$$\begin{aligned}312 &= 3\times 97+21\\ 97 &= 4\times 21+13\\ 21 &= 1\times 13+8\\ 13 &= 1\times 8+5\\ 8 &= 1\times 5+3\\ 5 &= 1\times 3+2\\ 3 &= 1\times 2+1\\ 2 &= 2\times 1\end{aligned}$$

   we can get $\gcd(312,97)=1$. By extended Euclidean algorithm, from $s_0=1, s_1=0, t_0=0, t_1=1$, and for $j=2,3,4,5,6,7,8$, we have

$$s_j = s_{j-2} - q_{j-1}s_{j-1},\ t_j = t_{j-2} - q_{j-1}t_{j-1}$$

   Finally, we can get $s_8=37, t_8=-119$. Thus, $1=\gcd(312,97)=312\times 37+97\times(-119)$. So 37 is the inverse of $312 mod 97$. Therefore, $37\times 312x \equiv 37\times 3(mod\ 97) \implies x\equiv 111(mod\ 79)$.

9 Q9

Let domain $A=\{0,...m-1\}$ and codomain $B=\{0,...,m-1\}$

- Injective.
  Suppose for any $x,y\in A$, we have $f(x)=f(y)$, then

$$\begin{aligned}&(ax)\ mod\ m = (ay)\ mod\ m\\ &\implies ax\equiv ay(mod\ m)\ (by\ definition\ of\ congruence)\\ &\implies x\equiv y(mod\ m)\ (since\ gcd(a,m)=1)\\ &\implies x=y\ (since\ x<m\ and\ y<m)\end{aligned}$$

  So f is injective.

- Surjective.
  Since $|A|=|\{0,...m-1\}|=m$ and $f:A\mapsto B$ is injective, then $|f(A)|=|\{f(0),...,f(m-1)\}|=m$. Since $|B|=|\{0,...m-1\}|=m$ and $f(A)\subseteq B$, we have $f(A)=B$, i.e., f is surjective.

10 Q10

For n being even, i.e., $n = 2k$ with k an integer. Then $n^2 = 4k^2$, so $n^2 \equiv 0(mod\ 4)$.
For n being odd, i.e., $n = 2k + 1$ with k an integer. Then $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, so $n^2 \equiv 1(mod\ 4)$.
After all, $n^2 \equiv 0$ or $1(mod\ 4)$. ■

11 Q11

Suppose there are two integers a and b, then from Q10, we have $n^2 \equiv 0(mod\ 4)$ if n is even and $n^2 \equiv 1(mod\ 4)$ if n is odd, where n is an integer. We can start from the following situations:

- Both a and b are even. Then $a^2 \equiv 0(mod\ 4)$ and $b^2 \equiv 0(mod\ 4)$. By the property of congruence, we have $a^2 + b^2 \equiv 0 + 0(mod\ 4)$, i.e., $a^2 + b^2 \equiv 0(mod\ 4)$.
- Both a and b are odd. Then $a^2 \equiv 1(mod\ 4)$ and $b^2 \equiv 1(mod\ 4)$. By the property of congruence, we have $a^2 + b^2 \equiv 1 + 1(mod\ 4)$, i.e., $a^2 + b^2 \equiv 2(mod\ 4)$.
- One is even and the other is odd in a and b. There is no change that we suppose a is odd and b is even (if not in real situation, then exchange the value of a and b), then $a^2 \equiv 1(mod\ 4)$ and $b^2 \equiv 0(mod\ 4)$. By the property of congruence, we have $a^2 + b^2 \equiv 1 + 0(mod\ 4)$, i.e., $a^2 + b^2 \equiv 1(mod\ 4)$.

Thus, $a^2 + b^2 \equiv 0$ or 1 or $2(mod\ 4)$. However, for $m = 4k + 3$ with $k \in \mathbb{Z} \wedge k \geq 0$, i.e., $m \equiv 3(mod\ 4)$, it is clear that $a^2 + b^2$ and m are not in the same residue class (mod 4). So, m will not be the sum of the squares of two integers. ■

12 Q12

To prove the proposition in the problem, we only need to prove its contrapositive: for positive integers a and m, if a has the inverse modulo m, i.e., $ax \equiv 1(mod\ m)$ has solution of x, then $gcd(a, m) = 1$.
Suppose there is a solution x_0 of $ax \equiv 1(mod\ m)$, then $ax_0 - 1 = km$ for $k \in \mathbb{Z}$. Thus, $1 = ax_0 - km$. By the property of division, we have $gcd(a, m)|(ax_0 - km)$. So, $gcd(a, m)|1$, i.e., $gcd(a, m) = 1$. ■

13 Q13

The same as Q2.

14 Q14

By definition, since $a \equiv b \mod m$, we have $m|(a - b)$, i.e. $\exists k \in \mathbb{Z}, (a - b) = km$, which means $a = km + b$.
By the lemma of Euclidean algorithm, we have $\gcd(a, m) = \gcd(m, b) = \gcd(b, m)$. ■

15 Q15

Since $x \equiv 3(mod\ 6)$, we have $\exists t \in \mathbb{Z}^+, x = 3 + 6t$. Substituting into $x \equiv 4(mod\ 7)$, we have

$$3 + 6t \equiv 4(mod\ 7)$$

which can be simplified as $t \equiv 6(mod\ 7)$, i.e., $\exists k \in \mathbb{Z}^+, t = 6 + 7k$. Therefore, $x = 3 + 6t = 3 + 6(6 + 7k) = 39 + 42k$, i.e., $x \equiv 39(mod\ 42)$.

16 Q16

Since $x \equiv 5(mod\ 6)$, we have $\exists t \in \mathbb{Z}^+, x = 5 + 6t$. Substituting into $x \equiv 3(mod\ 10)$, we have

$$5 + 6t \equiv 3(mod\ 10)$$

which can be simplified as $t \equiv 3(mod\ 5)$, i.e., $\exists k \in \mathbb{Z}^+, t = 3+5k$. Thus, $x = 5+6t = 5+6(3+5k) = 23+30k$. Similarly, substituting into $x \equiv 8(mod\ 15)$, we have

$$23 + 30k \equiv 8(mod\ 15)$$

which can be simplified as $k \equiv 0(mod\ 1)$. By back substituting, we have $x \equiv 23(mod\ 30)$.

17 Q17

Since $de \equiv 1(mod\ (p-1)(q-1))$, we have

$$\exists k \in \mathbb{Z}, de = 1 + k(p-1)(q-1)$$

Since $C \equiv M^e(mod\ pq)$, we have

$$C^d \equiv (M^e)^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)}(mod\ pq)$$

Since p and q are primes, and $gcd(M, pq) > 1$, then we have $M = lp$ for $l \in \mathbb{Z}$ and $gcd(M, q) = 1$. (Or $M = lq$ for $l \in \mathbb{Z}$ and $gcd(M, p) = 1$, which has the same analysis).
By Fermat's little theorem, we have

$$M^{q-1} \equiv 1(mod\ q)$$

Thus,

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M(mod\ q)$$

By the property of congruence, we have

$$\exists t \in \mathbb{Z}, M^{ed} = M + tq, i.e., (lp)^{ed} = lp + tq$$

Since $p|lp$ and $p|(lp)^{ed}$, we have $p|tq$. Since $gcd(p, q) = 1$, by the proprety of division, we have $p|t$. So we can let $t = rp$ for $r \in \mathbb{Z}$. Then

$$M^{ed} = M + tq = M + rpq$$

Therefore, $C^d \equiv M^{ed} \equiv M(mod\ pq)$. ∎