Assignment3

12011517 李子南

Q1.

If $a|b$, then $\exists c \in Z(ac = b)$

If $b|a$, then $\exists d \in Z(bd = a)$

Therefore $\exists c \in Z \exists d \in Z(bcd = b)$

$bd = 1$

$b = 1, d = 1 or b = -1, d = -1$

Therefore $a = b\ or\ a = -b$

Q2.

(a)$1768/16 = 110 \ldots\ 8$

$110/16 = 6 \ldots\ 14$

$(1768)_{10} = 6E8$

(b)$1 * 2^4 + 1 * 2^2 + 1 = (21)_{10}$

$21/8 = 2 \ldots\ 5$

$(10101)_2 = (25)_8$

(c)$(3)_{16} = (0011)_2$

$(B)_{16} = (1011)_2$

$(5)_{16} = (0101)_2$

$(A)_{16} = (1010)_2$

$(3B5A)_{16} = (0011101101011010)_2$

Q3.

(a)2

(b) 2 3 5 7

(c)2 3 5

Q4.

(a)$267/79 = 3 \ldots\ 30$

$gcd(267, 79) = gcd(79, 30)$

$79/30 = 2 \ldots\ 19$

$gcd(79, 30) = gcd(30, 19)$

$30/19 = 1 \ldots\ 11$

$gcd(30, 19) = gcd(19, 11)$

$19/11 = 1 \ldots\ 8$

$gcd(19, 11) = gcd(11, 8)$

$11/8 = 1 \ldots\ 3$

$gcd(11, 8) = gcd(8, 3)$

$8/3 = 2 \dots\ 2$

$gcd(8,3) = gcd(3,2) = 1$

Therefore $gcd(267,79) = 1$, they are relatively prime

(b)$1 = 3 - (8 - 2*3) = 3*3 - 8$

$3*3 - 8 = 3*(11 - 1*8) - 8 = 3*11 - 4*8$

$3*11 - 4*8 = 3*11 - 4*(19 - 11) = 7*11 - 4*19$

$7*11 - 4*19 = 7*(30 - 19) - 4*19 = 7*30 - 11*19$

$7*30 - 11*19 = 7*30 - 11*(79 - 2*30) = 29*30 - 11*79$

$29*30 - 11*79 = 29*(267 - 3*79) - 11*79 = 29*267 - 98*79$

Therefore $1 = 29*267 - 98*79$

Q5.

Assume $a = p_1^{a_1} p_2^{a_2} \dots\ p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots\ p_n^{b_n}$, $y = p_1^{y_1} p_2^{y_2} \dots\ p_n^{y_n}$

Then $gcd(a,b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \dots\ p_n^{min(a_n,b_n)}$

$gcd(gcd(a,b),y) = p_1^{min(a_1,b_1,y_1)} p_2^{min(a_2,b_2,y_2)} \dots\ p_n^{min(a_n,b_n,y_n)}$

$gcd(a,y) = d_1 = p_1^{min(a_1,y_1)} p_2^{min(a_2,y_2)} \dots\ p_n^{min(a_n,y_n)}$

$gcd(b,y) = d_2 = p_1^{min(b_1,y_1)} p_2^{min(b_2,y_2)} \dots\ p_n^{min(b_n,y_n)}$

$gcd(d_1,d_2) = p_1^{min(a_1,b_1,y_1)} p_2^{min(a_2,b_2,y_2)} \dots\ p_n^{min(a_n,b_n,y_n)}$

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

Q6.

Assume $ax + by = 1$

Then $2 = 2ax + 2by$

$2ax + 2by = (a-b)x + (a+b)x + (b-a)y + (b+a)y = (b-a)(y-x) + (a+b)(x+y)$

Therefore $gcd(b+a, b-a) = 2$

Q7.

(a)Let $a = 2, p = 4$

$2^3 = 8\%4 = 0$

(b)1.

$\because gcd(302,11) = 1, 11\ is\ prime$

According to Fermat's little rule

$302^{10}\%11 = 1$

$302^{302}(mod\ 11) = (302^{10}\%11)^{30} * (302^2\%11)$

$302 \equiv 5(mod\ 11)$

$302^{302}(mod\ 11) = (302^{10}\%11)^{30} * (5^2\%11) = 3$

2.

$4762\%13 = 4$

$4762^{5367}\%13 = 4^{5367}\%13$

$\because gcd(4,13) = 1, 13\ is\ prime$

According to Fermat's little rule

$4^{12}\%13 = 1$

$4^{5367}\%13 = 4^{5367 mod 12}\%13 = 4^3\%13 = 12$

3.

$\because gcd(2, 523) = 1, 523\ is\ prime$

According to Fermat's little rule

$2^{522}\%523 = 1$

$2^{39674}\%523 = 2^{39674 mod 522}\%523 = 2^2 = 4$

Q8.

(a)$79\ is\ prime$

$gcd(267, 79) = 1$

$1 = 3 - 1 * 2 = 3 * 3 - 8 = 3 * 11 - 4 * 8 = 7 * 11 - 4 * 19 = 7 * 30 - 11 * 19 = 29 * 30 - 11 * 79 = 29 * 267 - 98 * 79$

$267 * 29 \equiv 1(mod\ 79)$

$29 * 267 * x \equiv 3 * 29(mod\ 79)$

$x \equiv 8(mod\ 79)$

(b)$97\ is\ prime$

$gcd(312, 97) = 1$

$1 = 3 - 2 = 2 * 3 - 5 = 2 * 8 - 3 * 5 = 5 * 8 - 3 * 13 = 5 * 21 - 8 * 13 = 37 * 21 - 8 * 97 = 37 * 312 - 119 * 97$

$312 * 37 \equiv 1(mod\ 97)$

$312 * 37 * x \equiv 3 * 37(mod\ 97)$

$x \equiv 14(mod\ 97)$

Q9.

Let $S = \{0, \ ... \ , m-1\}$ denote domain

$x, y \in S$

$ax\ mod\ m = ay\ mod\ m$

$ax \equiv ay(mod\ m)$

Because $gcd(a, m) = 1$

Therefore $x \equiv y(mod\ m)$

Thus $m|x - y$

$0 \leq (x - y) < m$

Therefore it's only possible when $x = y$, $f(x)$ is injective.

Because $gcd(a, m) = 1$

Let b Be the inverse of a mod m

$ab \equiv 1(mod\ m)$

Let $z \in S$

$x = bz(mod\ m)$

$ax \equiv abz \equiv z(mod\ m)$

Because $z \in S$

$f(x) = z$

$f(x)$ is onto.

Therefore $f(x)$ is bijective.

Q10.

If $n = 2k,\ k \in Z$

$n^2 = 4k^2$

Therefore $n^2(mod\ 4) = 4k^2(mod\ 4) = 0$

If $n = 2k - 1, k \in Z$

$n^2 = 4k^2 - 4k + 1$

Therefore $n^2(mod\ 4) = 4k^2 - 4k + 1(mod\ 4) = 1$

Therefore $n^2 \equiv 0\ or\ 1(mod\ 4)$

Q11.

From Q10 we know

$a^2 + b^2 \equiv 0\ or\ 1\ or\ 2(mod\ 4)$

$4k + 3 \equiv 3(mod\ 4)$

$4k + 3 \not\equiv a^2 + b^2(mod\ 4)$

Therefore $4k + 3$ is not the sum of the squares of integers

Q12.

Assume $\exists \overline{a} \in Z(a\overline{a} \equiv 1(mod\ m))$

$a\overline{a} + tm = 1$

$\because gcd(a, m) \neq 1$

Then $\exists(d \in Z \land d > 1)(d|a \land d|m)$

$a = dp(p \in Z), m = dq(q \in Z)$

$d(\overline{a}p + tq) = 1$

Therefore $d = 1\ or\ -1$

It's contradict with the assumption.

Therefore a does not have an inverse modulo m.

Q13.

(a)$1768/16 = 110 \ldots\ 8$

$110/16 = 6 \ldots\ 14$

$(1768)_{10} = (6E8)_{16}$

(b)$(10101)_2 = 1 + 1 * 2^2 + 1 * 2^4 = (21)_{10}$

$21/8 = 2 \ldots\ 5$

$(10101)_2 = (25)_8$

$(10101)_2 = (25)_8$

(c)$(3)_{16} = (0011)_2$

$(B)_{16} = (1011)_2$

$(5)_{16} = (0101)_2$

$(A)_{16} = (1010)_2$

$(3B5A)_{16} = (0011101101011010)_2$

Q14.

Assume $c = gcd(a, m)$

Then we have $c|a$ and $c|m$

$\exists p, q \in Z((pc = a) \land (qc = m))$

$\because a \equiv b(mod\ m)$

$\exists k \in Z(a - b = km)$

So $b = c(p - kq)$

Thus $c|b$

Therefore $gcd(a, m) \leq gcd(b, m)$

By an analogous argument we can get $gcd(b, m) \leq gcd(a, m)$

Therefore $gcd(a, m) = gcd(b, m)$

Q15.

$\because x \equiv 3(mod\ 6)$

$x = 6k + 3, k \in Z$

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

$6k \equiv 1(mod\ 7)$

$k \equiv 6(mod\ 7)$

$k = 7q + 6, q \in Z$

$x = 6(7q + 6) + 3 = 42q + 39$

$x \equiv 39(mod\ 42)$

Q16.

Because $6, 10, 8$ are not relative prime.

$x \equiv 5(mod\ 6), x \equiv 3(mod\ 10), x \equiv 8(mod\ 15)$ can be convert to $x \equiv 1(mod\ 2), x \equiv 2(mod\ 3), x \equiv 3(mod\ 5)$

Using Chinese remainder Theorem

$M_1 = 15, M_2 = 10, M_3 = 6$

$M_1 * 1 \equiv 1(mod\ 2), M_2 * 1 \equiv (mod\ 3), M_3 * 1 \equiv (mod\ 5)$

$x \equiv 1 * 15 * 1 + 2 * 10 * 1 + 3 * 6 * 1 = 53 \equiv 23(mod\ 30)$

Q17.

When $gcd(M, pq) > 1$

We have $gcd(M, p) = p, gcd(M, q) = q\ or\ gcd(M, p) = 1, gcd(M, q) = q\ or\ gcd(M, p) = p, gcd(M, q) = 1$

$de \equiv 1(mod\ (p - 1)(q - 1))$

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

WLOG, consider the case $gcd(M, p) = p, gcd(M, q) = 1$

$C^d \equiv M^{1+k(p-1)(q-1)}(mod\ p) \equiv 0(mod\ p) \equiv M(mod\ p)$

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

Since $gcd(p, q) = 1$, $C^d \equiv M(mod\ n)$ by Chinese remainder Theorem.