CS215 Ass3 12310401 王子恒

Q.1 a) $8085 = 5 \times 1617$

$= 3 \times 5 \times 539$

$= 3 \times 5 \times 7 \times 77$

$= 3 \times 5 \times 7^2 \times 11$

b) $= 2 \times 3 \times 2^2 \times 5 \times (2 \times 3) \times 7 \times 2^3 \times 3^2 \times (2 \times 5)$

$= 2^8 \times 3^4 \times 5^2 \times 7$

Q.2. $a = k_1 d_1$ $\quad b = k_2 d_2$ $\quad y = k_3 d_1 d_2$

$\gcd(k_1, k_3 d_2) = \gcd(k_2, k_3 d_1) = 1$

$\Rightarrow \gcd(k_1, d_2) = 1 \quad \gcd(k_2, d_1) = 1$

thus $\gcd(a,b) = \gcd(k_1 d_1, k_2 d_2) = \gcd(k_1, k_2) \cdot \gcd(d_1, d_2)$

Thus $\gcd(d_1, d_2) \mid \gcd(a,b)$

And: $y = k_3 d_1 d_2 = k_3 \gcd(d_1, d_2) \cdot \operatorname{lcm}(d_1, d_2)$

Therefore $\gcd(d_1, d_2) \mid y$

$\gcd(\gcd(a,b), y) = x_1 \gcd(a,b) + x_2 y$ (Bezout's identity)

Hence $\gcd(d_1, d_2) \mid \gcd(\gcd(a,b), y)$.

---

suppose $k \mid \gcd(a,b) \quad k \mid y$

$\Rightarrow k \mid a,\ k \mid b,\ k \mid y$

$\Rightarrow k \mid \gcd(a,y) = d_1, \quad k \mid \gcd(b,y) = d_2$

$\Rightarrow k \mid \gcd(d_1, d_2)$

$\Rightarrow \gcd(\gcd(a,b), y) \mid \gcd(d_1, d_2)$

Hence $\gcd(\gcd(a,b), y) = \gcd(d_1, d_2)$.

Q4. $a \cdot \gcd(b,c) = (x_1 b + x_2 c)a = x_1 ab + a x_2 c$

if $c \mid (a \cdot b)$ then $c \mid x_1 ab \Rightarrow c \mid x_1 ab + a x_2 c \Rightarrow c \mid (a \cdot \gcd(b,c))$

Q5. $312 = 97 \times 3 + 21$

$\Rightarrow 21x \equiv 3 \pmod{97}$

$21y \equiv 1 \pmod{97}$

$97 = 21 \times 4 + 13$

$21 = 13 + 8$

$13 = 8 + 5$

$8 = 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$2 = 1 \times 2 + 0.$

$1 = 3 - 2$

$= 3 \times 2 - 5$

$= 8 \times 2 - 5 \times 3$

$= 8 \times 5 - 13 \times 3$

$= 21 \times 5 - 13 \times 8$

$= 21 \times \underline{\underline{37}} \quad 97 \times 8$

$\therefore 21 \times 37 x \equiv 3 \times 37 \mod 97$

$x \equiv 111 \mod 97$

$x \equiv 14 \mod 97$

Q.6. (a) $a = 4, \quad b = 3, \quad c = 2, \quad m = 2.$

$ac \equiv bc \equiv 0 \pmod 2$

$a \equiv 0 \pmod 2$

$b \equiv 1 \pmod 2$

(b)

$2 \equiv 5 \mod 3.$

$3 \equiv 0 \mod 3$

$2^3 \equiv 2 \mod 3$

$5^0 \equiv 1 \mod 3$

Q.7. injection:

if $f(x)=f(y)$, then: $a\cdot x \bmod m = a\cdot y \bmod m$

$\Rightarrow \quad a\cdot x \equiv a\cdot y \mod m$

since $\gcd(a,m)=1$, then we have an a^{-1} that $a\cdot a^{-1}\equiv 1 \mod m$

$\Rightarrow \quad a^{-1}a\cdot x \equiv a^{-1}\cdot a\cdot y \mod m$

$x \equiv y \mod m$

therefore $m \mid x-y$

since $-(m-1) < x-y < m-1$ thus $x-y=0$ $x=y$

surjection:

we should proof that for every $y\in\{0,\cdots m-1\}$, there is an $x\in\{0,\cdots m-1\}$

let $f(x)=y$, which means $a\cdot x \bmod m = y$

which means $a\cdot x \equiv y \mod m$.

since $a^{-1}a\cdot x \equiv a^{-1}y \mod m$

$x \equiv a^{-1}y \mod m$.

we can choose the distinct x in $\{0,\cdots m-1\}$ that $x\equiv a^{-1}y \mod m$

Thus, the f is injective and surjective, f is bijective.

Q.8. (a)

	231
1	115
1	57
1	28
0	14
0	7
1	3
1	1
1	0

$(231)_{10} = (11100111)_2$

(b)

	4532
0	2266
0	1133
1	561
1	280
0	140
0	70
0	35
1	17
1	8
0	4
0	2
0	1
1	0

$(4532)_{10} = (1000110001100)_2$

Q.9. (1) $f(cm) = c + a_1 \cdot cm + a_2 \cdot c^2 m^2 + \cdots + a_{t-1} \cdot c^{t-1} \cdot m^{t-1} + c^t m^t$

since every part of the polynomial is a multiple of c.

Thus $f(cm)$ is a multiple of c.

(2) since $f(cm)$ is a multiple of c $c>1$

and $f(cm) > f(0) = c$ thus $f(cm)$ is not a prime.

Besize m can choose infinitely thus there are infinitely many $f(cm) \in Z$ that are not primes

(3) if $c=1$

$f(n) = 1 + a_1 n + a_2 n^2 + \cdots + n^{t-1} + n^t$

suppose $f(n_0) = p$ is a prime

then $f(n_0 + kp) = 1 + a_1 (n_0 + kp) + a_2 (n_0 + kp)^2 + \cdots + (n_0 + kp)^t$

$= 1 + a_1 n_0 + a_2 n_0^2 + \cdots + n_0^t + q \cdot p$ for some q

$= f(n_0) + q \cdot p$

$= (1+q) p$ is not a prime.

since k can choose infinitly, there must be a composite that $q \neq 1$
there must a composite number $f(n_0 + kp)$ for some k.

If $c > 1$ from (2), there are infinite $f(n)$ that not not prime.

In a nut shell, for every non-constant polynomial f, the must be an $n \in N$ such that $f(n)$ is not prime.

Q.10. $\gcd(a, m) = 1$

$1 = xa + ym$.

suppose there are two element $p, q \in [0, m-1)$.

$pa \equiv 1 \mod m$, $qa \equiv 1 \mod m$.

$\Rightarrow m \mid pa - 1$ $m \mid qa - 1$

$\Rightarrow m \mid (p-q) a$

since $m \nmid a$

then $m \mid (p-q)$

$-(m-1) < p-q < (m-1)$ thus $p-q = 0$ $p = q$.

the inverse of a modulo is unique modulo m.

Q.11. suppose there are only finitely many primes in the form $4k+3$

then $Q = 4q_1q_2\cdots q_n - 1$ can be written in multiple of $q_1 \cdots q_n$

$= 4(q_1q_2\cdots q_n - 1) + 3$

if $q_j \mid Q$ then $q_j \mid 4q_1q_2\cdots q_n - Q = 1$.

which is not impossible.

Thus we can get a new prime not in $q_1 \cdots q_n$ that

either be the prime composite of Q or Q.

if Q is prime, we get a new prime different to $q_1 \cdots q_n$

if Q is not prime, then Q has at least one prime factor not in the list $q_1 \cdots q_n$

because the remainder when Q is divided by q_j is $q_j - 1$ and $q_j - 1 \neq 0$. Because all odd primes are either $4k+1$ or $4k+3$, and the product of primes of the form $4k+1$ is $(4k+1)(4m+1) = 4(4km+k+m)+1$, thus Q must have a factor as $4k+3$ not in $q_1 \cdots q_n$.

Hence there are infinitely many primes in the form $4k+3$.

Q.12 (1) if $n \equiv 0 \pmod 4$ then $n = 4k$ $n^2 \equiv 0 \pmod 4$

if $n \equiv 1 \pmod 4$ then $n = 4k+1$ $n^2 \equiv 1 \pmod 4$

if $n \equiv 2 \pmod 4$ then $n = 4k+2$ $n^2 \equiv 0 \pmod 4$

if $n \equiv 3 \pmod 4$ then $n = 4k+3$ $n^2 \equiv 1 \pmod 4$

Thus if n is an integer then $n^2 \equiv 0$ or $1 \mod 4$

(2) Accorting to a we can get that

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

thus $n_1^2 + n_2^2 = \begin{cases} 4k_1 + 4k_1 = 4(k_1+k_2) \\ 4k_1 + 4k_2+1 = 4(k_1+k_2)+1 \\ 4k_1+1+4k_2+1 = 4(k_1+k_2)+2 \end{cases}$

None of them is in the form $4k+3$.

Thus m is not the sum of the squares of two integers.

Q-13. (a) Let p be a prime, and let x be an integer such that $x \not\equiv 0 \mod p$. Then $x^{p-1} \equiv 1 \pmod p$.

(b) $p = 4$ $\quad x = 2$ $\quad x^{p-1} = 2^3 \equiv 0 \mod 4$

(c) $302^{302} = 302^{30 \times 10} \times 302^2 = (302^{10})^{30} \cdot 302^2 = 1^{30} \cdot 302^2 \equiv 5^2 \equiv 3 \mod 11$

$4762^{5367} = 4762^{447 \times 12} \times 4762^3 = 4762^3 \equiv 4^3 \equiv 12 \mod 13$

$2^{39674} = 2^{552 \times 76} \times 2^{146} = (2^{10})^{14} \times 2^6 = (501)^{14} \times 64 \mod 523$

$= 484^7 \times 64 = 475^3 \times 484 \times 64 = 212 \times 303 \times 64 = 493 \times 303$

$= 324 \mod 523.$

Q.14. Because $m_i | a-b$, m_i are relative prime

then $m_1 m_2 \cdots m_n | a-b$ which means $a \equiv b \mod m$.

Q.15. $x \equiv 3 \mod 6$

$x \equiv 4 \mod 7$

$m = 42 \quad M_1 = 7 \quad M_2 = 6.$

$7 \equiv 1 \mod 6 \quad y_1 = 1$

$6 \cdot 6 \equiv 1 \mod 7 \quad y_2 = 6$

$x = 3 \times 7 \times 1 + 4 \times 6 \times 6 = 21 + 144 = 165 \equiv 39 \mod 42$

back substitution

$x = 6k + 3 \mod 6 \quad 6k+3 \equiv 4 \mod 7$

$6k \equiv 1 \mod 7$

$k \equiv 6 \mod 7$

$k = 7t + 6$

$x = 6(7t+6) + 3$

$= 42t + 39$

$x \equiv 39 \mod 42.$

Q.16

$$n \equiv 1 \mod 2.$$
$$n \equiv 0 \mod 3.$$
$$n \equiv 1 \mod 4.$$
$$n \equiv 4 \mod 5.$$
$$n \equiv 3 \mod 6$$
$$n \equiv 0 \mod 7.$$
$$n \equiv 1 \mod 8$$
$$n \equiv 0 \mod 9.$$

$$x = 5a+4 \equiv 0 \mod 7.$$
$$5a \equiv 3 \mod 7$$
$$a \equiv 2 \mod 7.$$
$$x = 5(7b+2)+4$$
$$= 35b+14 \equiv 1 \mod 8.$$
$$35b \equiv 3 \mod 8$$
$$3b \equiv 3 \mod 8.$$
$$b \equiv 1 \mod 8.$$
$$x = 35(8c+1)+14$$
$$= 280c+49 \equiv 0 \mod 9$$
$$280c \equiv 5 \mod 9$$
$$c \equiv 5 \mod 9$$
$$x = 280(9d+5)+49$$
$$= 2520d+1449$$

the number of balls is $n = 2520d + 1449$ $n = 0, 1, 2 \cdots$

Q.17.

$$ax_0 + c \equiv 7 \mod 11$$
$$7a + c \equiv 4 \mod 11$$
$$4a + c \equiv 6 \mod 11$$
$$\Rightarrow \begin{cases} a = 3 \\ c = 5 \end{cases}$$

next: $6 \times 3 + 5 = 23 \equiv 1 \mod 11$

next is 1.

Q.18. Because $\gcd(n, x) = \gcd(n, n-x)$ $(n > x)$, every time x coprime to n there must be a number $n-x$ also coprime to n. Thus $\varphi(n)$ is even when $n \geq 3$.

Q.19.

(a) $n = 91 = 7 \times 13$ $\varphi(n) = 6 \times 12 = 72$ $\gcd(72, 25) = 1$

$ed = 1275 \equiv 51 \mod 72$ not valid.

(b) $ed = 1225 \equiv 1 \mod 72$ valid

(c) $n = 84 = 2^2 \times 3 \times 7$ not valid

n is not two prime's multiplication

Q. 20. Because $\Phi(n) = (p-1)(q-1)$, $\lambda(n)$ is a factor of $\Phi(n)$

Assume. $\Phi(n) = k\lambda(n)$ $\quad ed' = t\lambda(n) + 1$

$$C^{d'} \equiv (M^e)^{d'} \equiv M^{ed'} = M^{1+t\lambda(n)} \quad \text{mod}(n).$$

$$C^{d'} \equiv M \cdot M^{\frac{t}{k}(p-1)(q-1)} \equiv M \cdot 1 \equiv M \quad \text{mod } p.$$

$$C^{d'} \equiv M \cdot M^{\frac{t}{k}(q-1)(p-1)} \equiv M \cdot 1 \equiv M \quad \text{mod } q$$

$$\therefore C^{d'} \equiv M \quad (\text{mod } pq).$$