Assignment 3

Q1. (a) $8085 = 3 \times 5 \times 7^2 \times 11$

(b) $10! = 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 \times 2 \times 5$

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

Q3. Let a, b, y have no more prime factors than $p_1, p_2 \cdots p_k$

$a = p_1^{e_{a1}} p_2^{e_{a2}} \cdots p_k^{e_{ak}} \quad b = p_1^{e_{b1}} p_2^{e_{b2}} \cdots p_k^{e_{bk}}$

$y = p_1^{e_{y1}} p_2^{e_{y2}} \cdots p_k^{e_{yk}}$

$\Rightarrow d_1 = \gcd(a, y) = p_1^{\min(e_{a1}, e_{y1})} p_2^{\min(e_{a2}, e_{y2})} \cdots p_k^{\min(e_{ak}, e_{yk})}$

$d_2 = \gcd(b, y) = p_1^{\min(e_{b1}, e_{y1})} p_2^{\min(e_{b2}, e_{y2})} \cdots p_k^{\min(e_{bk}, e_{yk})}$

$\gcd(d_1, d_2) = p_1^{\min(\min(e_{a1}, e_{y1}), \min(e_{b1}, e_{y1}))} p_2^{\min(\min(e_{a1}, e_{y1}), \min(e_{b2}, e_{y2}))}$

$\cdots p_k^{\min(\min(e_{ak}, e_{yk}), \min(e_{bk}, e_{yk}))}$

$= p_1^{\min(e_{a1}, e_{y1}, e_{b1})} p_2^{\min(e_{a2}, e_{y2}, e_{b2})} \cdots p_k^{\min(e_{ak}, e_{yk}, e_{bk})}$

And $\gcd(a, b) = p_1^{\min(e_{a1}, e_{b1})} p_2^{\min(e_{a2}, e_{b2})} \cdots p_k^{\min(e_{ak}, e_{bk})}$

$\gcd(\gcd(a, b), y) = p_1^{\min(\min(e_{a1}, e_{b1}), e_{y1})} p_2^{\min(\min(e_{a2}, e_{b2}), e_{y2})} \cdots$

$p_k^{\min(\min(e_{ak}, e_{bk}), e_{yk})}$

$= p_1^{\min(e_{a1}, e_{b1}, e_{y1})} p_2^{\min(e_{a2}, e_{b2}, e_{y2})} \cdots p_k^{\min(e_{ak}, e_{bk}, e_{yk})}$

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

Q4. Let $b = \gcd(b,c) \cdot m$, then $\gcd(m,c) = 1$

$c \mid a \cdot b \Rightarrow c \mid a \cdot \gcd(b,c) \cdot m$

then $c \mid (a \cdot \gcd(b,c))$

Q5. find 312's inverse (mod 97)

$\gcd(312, 97) = 1$

$312 = 97 \times 3 + 21$

$97 = 21 \times 4 + 13$

$21 = 13 \times 1 + 8$

$13 = 8 \times 1 + 5$

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2$

$\Rightarrow$

$1 = 3 - 2 \times 1$

$= 2 \times 3 - 5$

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

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

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

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

$= 13 \times 97 - 60 \times 21$

$= -60 \times 312 + 193 \times 97$

$\Rightarrow 312 \times (-60) \equiv 1 \pmod{97}$

$x \equiv -60 \times 3 \equiv 14 \pmod{97}$

Q6. (a) $a=1$, $b=2$ $c=4$, $m=4$

$ac \equiv bc \equiv 0 \pmod{m}$

$a \not\equiv b \pmod{m}$

(b) $a=5$ $b=2$ $c=4$ $d=1$ $m=3$

$a \equiv b \equiv 2 \pmod{m}$ $c \equiv d \equiv 1 \pmod{m}$

$a^c \equiv 1 \pmod{m}$ $b^d \equiv 2 \pmod{m}$

$\Rightarrow a^c \not\equiv b^d \pmod{m}$

Q7. prove injective: assume $f(x) = f(y)$

$ax \equiv ay \pmod m \Rightarrow m \mid a(x-y)$

for $\gcd(a, m) = 1 \Rightarrow m \mid x-y$

$x, y \in \{0, \dots, m-1\}$ $\quad -(m-1) < x-y < m-1$

then $x-y = 0 \quad x = y$

prove surjective:

for finite sets, if $|A| = |B|$ and has one-to-one function $f: A \to B$, then f is also onto.

then we prove $|A| = |B|$

$B \subseteq A$, then we only need to prove $A \subseteq B$.

when $x \neq y$, $f(x) \neq f(y)$, which was proved above by contrapositive proof.

Therefore $|A| = |B|$, then onto.

f is bijection.

Q8. (a) $231 = 2 \times 115 + 1$

$115 = 2 \times 57 + 1$

$57 = 2 \times 28 + 1$

$28 = 2 \times 14 + 0$

$14 = 2 \times 7 + 0$

$7 = 2 \times 3 + 1$

$3 = 2 \times 1 + 1$

$1 = 2 \times 0 + 1$

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

(b) $4532 = 2 \times 2266 + 0$
$2266 = 2 \times 1133 + 0$
$1133 = 2 \times 566 + 1$
$566 = 2 \times 283 + 0$
$283 = 2 \times 141 + 1$
$141 = 2 \times 70 + 1$
$70 = 2 \times 35 + 0$
$35 = 2 \times 17 + 1$
$17 = 2 \times 8 + 1$
$8 = 2 \times 4 + 0$
$4 = 2 \times 2 + 0$
$2 = 2 \times 1 + 0$
$1 = 2 \times 0 + 1$

then
$(4532)_{10} = (1000110110100)_2$

Q9. (1) if $m=0$ $f(cm) = f(0) = c$

$c \mid c \Rightarrow f(cm)$ is a multiple of c

if $c=0$ $f(cm) = f(0) = c = 0$

$\Rightarrow f(cm)$ is a multiple of c

if $cm \neq 0$, $f(cm) = c + a_1 cm + a_2 (cm)^2 + \cdots + a_{t-1}(cm)^{t-1} + (cm)^t$
m is integer
$c \mid c$, $c \mid a_1 cm$, $c \mid a_2 (cm)^2$ ... $c \mid (cm)^t$

$\Rightarrow c \mid f(cm)$

So $f(cm)$ is a multiple of c for all cases.

(2) from (1) we prove $c \mid f(cm)$

when $c > 1$, $f(cm)$ can be divided by c

Then we only need to prove there are infinite cm

build a bijective , $f: \mathbb{Z} \to \mathbb{Z}$ $f = cm$

then there are infinite cm, so there are infinitely many $f(n) \in \mathbb{Z}$ that are not primes

(3) if $c=0$ $f(n) = a_1 n + a_2 n^2 + \cdots + a_{t-1} n^{t-1} + n^t$

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

$n \mid f(n)$ for any $n \geq 2$; when $n \geq 2$ $f(n)$ is not prime

if $c=1$:

when $f(1) = p$ is a prime , then $p \mid f(1)$

$f(1+p) = 1 + a_1(1+p) + \cdots + a_{t-1}(1+p)^{t-1} + (1+p)^t$

$f(1) = 1 + a_1 + \cdots + a_{t-1} + 1$

$f(1+p) - f(1) = w_1 p + w_2 p^2 + \cdots + w_{t-1} p^{t-1} + p^t$

substract all constant term

then $f(1+p) - f(1) = p(w_1 + w_2 p + \cdots + w_{t-1} p^{t-2} + p^{t-1})$

$f(1+p) - f(1) \equiv 0 \pmod{p}$

$\Rightarrow f(1+p) \equiv 0 \pmod{p} \Rightarrow p \mid f(1+p)$

$f(1+p)$ is not prime.

when $f(1) = p$ is not prime, then we find it.

if $c > 1$, we prove it in (2)

Therefore , the proposition holds .

Q10. Prove by contradiction

Assume that the inverse of a modulo m is not unique

then $ax \equiv 1 \pmod m$, $ay \equiv 1 \pmod m$ and $x, y \in \{1, 2, \cdots m-1\}$

$\Rightarrow m \mid ax - ay$, $m \mid a(x-y)$

for $\gcd(m, a) = 1 \Rightarrow m \mid x-y$

$z - m \leq x - y \leq m-2 \Rightarrow x - y = 0 \quad x = y$

$\Rightarrow$ Therefore, the inverse is unique

Q11. Prove by contradiction

Assume that there aren't infinite $4k+3$ primes,

then we can find the largest $4k+3$ prime.

Let $4k+3$ primes be $q_1, q_2 \cdots q_n$ in ascending order.

Considering $N = 4q_1 q_2 \cdots q_n - 1 \quad 2 \nmid N$

Then we prove N is a prime, assume N isn't a prime.

Then N can be defactor as $N = p_1 p_2 \cdots p_m$, p_i is odd prime

if for some p_i, $p_i = 4k+3$ $(k \in Z)$, then $\exists\, q_k = p_i$

for $q_1 \sim q_n$ cover all $4k+3$ primes,

then $q_k \nmid 4q_1 q_2 \cdots q_n - 1 \quad p_i \mid p_1 p_2 \cdots p_m$

leads to contradiction.

Then if for all p_i, $p_i = 4k+1$ $(k \in Z)$, then $p_i \equiv 1 \pmod 4$

$p_1 p_2 \cdots p_m \equiv 1 \pmod 4$. while $4q_1 q_2 \cdots q_n - 1 \equiv 3 \pmod 4$

leads to contradiction.

Therefore N con't be defactor, N is a prime.

⇒ There are infinite $4k+3$ primes

Q12. (1) prove by case

if $n=4k$ $k\in\mathbb{Z}$, $n^2=16k^2\equiv 0 \pmod 4$

if $n=4k+1$ $k\in\mathbb{Z}$, $n^2=16k^2+8k+1=4(4k^2+2k)+1$
$\equiv 1 \pmod 4$

if $n=4k+2$ $k\in\mathbb{Z}$, $n^2=4(2k+1)^2\equiv 0 \pmod 4$

if $n=4k+3$ $k\in\mathbb{Z}$, $n^2=16k^2+24k+9\equiv 4(4k^2+6k)+9$
$\equiv 1 \pmod 4$

⇒ $n^2 \bmod 4 = 1$ or 0

(2) from (1) we know $n^2 \bmod 4 = 1$ or 0

① $a^2\equiv 1 \pmod 4$, $b^2\equiv 1 \pmod 4$ then $a^2+b^2\equiv 2 \pmod 4$

② $a^2\equiv 1 \pmod 4$, $b^2\equiv 0 \pmod 4$ then $a^2+b^2\equiv 1 \pmod 4$

③ $a^2\equiv 0 \pmod 4$, $b^2\equiv 1 \pmod 4$ then $a^2+b^2\equiv 1 \pmod 4$

④ $a^2\equiv 0 \pmod 4$, $b^2\equiv 0 \pmod 4$ then $a^2+b^2\equiv 0 \pmod 4$

⇒ There are no a, b that $a^2+b^2 \bmod 4 = 3$

$a^2+b^2 \neq 4k+3$ for every integer a, b, k

Q13. (a) Let p be a prime, and let x be an integer
s.t. $x \not\equiv 0 \pmod p$, then $x^{p-1}\equiv 1 \pmod p$

(b) let $p=4$, $x=2$

use Fermat little theorem, $x^{p-1}\equiv 1 \pmod p$

but $2^3\equiv 0 \pmod 4$

(c)

$\gcd(302, 11) = 1$

$302^{11-1} \equiv 1 \pmod{11}$

$302^{302} = 302^{10 \times 30} \cdot 302^2$

$\equiv 302^2 \pmod{11}$

$\equiv 5^2 \pmod{11}$

$\equiv 3 \pmod{11}$

$\gcd(4762, 13) = 1$

$4762^{13-1} \equiv 1 \pmod{13}$

$4762^{5367} = 4762^{12 \times 447 + 3} \pmod{13}$

$\equiv 4762^3 \pmod{13}$

$\equiv 4^3 \pmod{13}$

$\equiv 12 \pmod{13}$

$\gcd(2, 523) = 1$

$2^{523-1} \equiv 1 \pmod{523}$

$2^{89674} = 2^{522 \times 76 + 2}$

$\equiv 2^2 \pmod{523}$

$\equiv 4 \pmod{523}$

Q14. Assume

$a \equiv a_1 \pmod{m_1}$ $\quad b \equiv a_1 \pmod{m_1}$

$a \equiv a_2 \pmod{m_2}$ $\quad b \equiv a_2 \pmod{m_2}$

$\vdots$ $\quad \vdots$

$a \equiv a_n \pmod{m_n}$ $\quad b \equiv a_n \pmod{m_n}$

$m_1, m_2, \cdots m_n$ are pairwise relatively prime

for CRT, we can find solution

$a \equiv y_1 M_1 a_1 + y_2 M_2 a_2 + \cdots + y_n M_n a_n \pmod{m}$

$b \equiv y_1 M_1 a_1 + y_2 M_2 a_2 + \cdots + y_n M_n a_n \pmod{m}$

where $M_i = \frac{m}{m_i}$, $y_i M_i \equiv 1 \pmod{m_i}$

for $\gcd(M_i, m_i) = 1$ then y_i has unique solution in $\mathbb{Z}_{m_i}$

$\Rightarrow a \equiv b \pmod{m}$

Q15. for CRT

$x \equiv 3 \pmod 6$

$x \equiv 4 \pmod 7$

$m = 6 \times 7 = 42$

$M_1 = 7 \quad M_2 = 6$

$\gcd(6,7) = 1$

$y_1 M_1 \equiv 1 \pmod 6 \Rightarrow y_1 = 1$

$y_2 M_2 \equiv 1 \pmod 7 \Rightarrow y_2 = 6$

$x \equiv 3 \times 1 \times 7 + 4 \times 6 \times 6 \equiv 165 \equiv 39 \pmod{42}$

$x = 39 + 42k \quad k \in \mathbb{Z}$

Q16.

$x \equiv 2 \pmod 1$

$x \equiv 0 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 4 \pmod 5$

$x \equiv 3 \pmod 6$

$x \equiv 0 \pmod 7$

$x \equiv 1 \pmod 8$

$x \equiv 0 \pmod 9$

$\Rightarrow$ we only need

$x \equiv 4 \pmod 5$

$x \equiv 0 \pmod 7$

$x \equiv 1 \pmod 8$

$x \equiv 0 \pmod 9$

pairwise prime

$m = 5 \times 7 \times 8 \times 9 = 2520$

$m_1 = 504 \quad m_2 = 360 \quad m_3 = 315 \quad m_4 = 280$

$4m_1 \equiv 1 \pmod 5 \quad 5m_2 \equiv 1 \pmod 7 \quad 3m_3 \equiv 1 \pmod 8$

$1m_4 \equiv 1 \pmod 9$

$x \equiv 504 \times 4 \times 4 + 360 \times 5 \times 0 + 315 \times 3 \times 1 + 280 \times 1 \times 0$

$\equiv 8064 + 945 \equiv 1449 \pmod{2520}$

$x = 2520k + 1449 \quad k \in \mathbb{N}$

Q17. $4 \equiv 7a+c \pmod{11}$

$6 \equiv 4a+c \pmod{11}$

$\Rightarrow -2 \equiv 3a \pmod{11}$

$\gcd(3,11)=1$

$\Rightarrow$ 3 has inverse $\pmod{11}$

$3 \times 4 \equiv 1 \pmod{11}$

$\Rightarrow a \equiv -2 \times 4 \equiv 3 \pmod{11}$

let $a = 11k+3$ $k \in \mathbb{Z}$

$4 \equiv 7(11k+3)+c \pmod{11}$

$4 \equiv 21+c \pmod{11}$

$c \equiv 5 \pmod{11}$

let $c = 11t+5$

$\Rightarrow x_4 = (ax_3+c) \pmod{11}$

$\equiv (11k+3) \times 6 + 11t + 5 \pmod{11}$

$\equiv 18+5 \pmod{11}$

$\equiv 1 \pmod{11}$ $\quad x_4 \in \{0,1,\dots,10\}$

$\Rightarrow x_4 = 1$

Q18. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, where p_i is prime, $e_i \geq 1$

$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_m^{e_m} - p_m^{e_m-1})$

$= p_1^{e_1-1} p_2^{e_2-1} \cdots p_m^{e_m-1} (p_1-1)(p_2-1)\cdots(p_m-1)$

if $\exists p_k$ is odd, then $2 \mid p_k - 1 \Rightarrow 2 \mid \phi(n)$

if no p_i is odd, then $n = 2^e$ for $n \geq 3$

$e \geq 2 \Rightarrow \phi(n) = 2^{e-1}(2-1) = 2^{e-1}$

$e-1 \geq 1 \Rightarrow 2 \mid 2^{e-1}$

$\Rightarrow n \geq 3$, $\phi(n)$ is even

Q19. (a) invalid

$91 = 7 \times 13$ $\phi(n) = (7-1) \times (13-1) = 72$

$\gcd(e, \phi(n)) = 1$ $ed \equiv 51 \not\equiv 1 \pmod{72}$

(b) valid

$ed \equiv 25 \times 49 \equiv 1 \pmod{72}$

(c) invalid

$n = 2^2 \times 3 \times 7$ not the multiple of two primes

Q20. Yes

for traditional RSA: $n = pq$ $\phi(n) = (p-1)(q-1)$

$\gcd(e, \phi(n)) = 1$ $ed \equiv 1 \pmod{\phi(n)}$

for this RSA system:

$\lambda(n) = \text{lcm}(p-1, q-1)$ $d'e \equiv 1 \pmod{\lambda(n)}$

$C = M^e \pmod{n}$

We need to prove $C^{d'} \bmod n = M$.

$C^{d'} = M^{ed'} \equiv M^{k\lambda(n)} \cdot M \pmod{n}$

① $n \mid M$ $C^{d'} \equiv M \equiv 0 \pmod{n}$ it holds

② $p \mid M$ $q \nmid M$

$C^{d'} \equiv M \equiv 0 \pmod{p}$ (1)

$C^{d'} \equiv M^{k\lambda(n)} \cdot M \pmod{q}$

for $\gcd(M, q) = 1 \Rightarrow$ $M^{q-1} \equiv 1 \pmod{q}$

$k\lambda(n) = k(q-1)t_1 = k(p-1)t_2$

$\Rightarrow c^{d'} \equiv (M^{q-1})^{kt} \cdot M \equiv M \pmod{q}$ (2)

for (1)(2) $c^{d'} \equiv M \pmod{n}$

③ $p \nmid M$ $q \mid M$ the same as ②

④ $p \nmid M, q \nmid M$ $\gcd(M, n) = 1$

$\Rightarrow c^{d'} \equiv M^{k(q-1)t_1} \cdot M \equiv M \pmod{q}$ (3)

$c^{d'} \equiv M^{k(p-1)t_2} \cdot M \equiv M \pmod{p}$ (4)

for (3)(4) then $c^{d'} \equiv M \pmod{n}$

Therefore, $c^{d'} \bmod n = M$ for all cases