Homework 5

Sun Kai

5110309061

1. (mod 11) 800^{35}

   $= 8^{35}*10^{35}*10^{35}$

   $= 8^{35}*(-1)^{35}*(-1)^{35}$

   $=8^{35}$

   $=8*8^{2}*8^{32}$

   $=8*9*9^{16}$

   $=6*4^{8}$

   $=6*5^{4}$

   $=6*3^{2}$

   $=10$

2. (a) Let a be the smallest non-negative which satisfies:

   $i = k*p + a$ ($k\in N$). Then i (mod p) equals a.

   (b) i (mod p) = (i+p) (mod p)

3. $\because x-y=5$

   $\therefore 3x-3y=1$

   $\because 3x+2y=1$

   $\therefore 5y=0$

   $\therefore y=0$

   $\therefore x=5, y=0$

4. (a) gcd(495, 210) = gcd(210, 75) = gcd(75, 60) = gcd(60, 15) = gcd(15, 0)=15

   (b)495=3*3*5*11

   210=2*3*5*7

   (c)Yes. From (b) we can see both 495 and 210 have 3*5=15, so (a) is correct.

5. ∵ 997 = 400*2+197

   400 = 197*2+6

   197=6*32+5

   6=5*1+1

   1=1*1+0

   ∴ 1=1*1+0

   =(6-5*1)

   =1*[6-(197-6*32)]

   =33*6-197

   =33*(400-197*2)-197

   =33*400-67*197

   =33*400-67*(997-400*2)

   =33*400-67*997+400*134

   =400*167-997*67

   ∴400*167-997*67=1

   ∴400*167=1 (mod 997)

$\therefore 400^{-1}=167 \pmod{997}$

6. gcd(a,b)*lcm(a,b)=a*b

   Proof: Let c = gcd(a,b)

   $\therefore$ c|a, c|b

   $\therefore$ $a|\frac{ab}{c}$, $b|\frac{ab}{c}$

   $\therefore$ $\frac{ab}{c}$ is the common multiple of a and b

   So the least common multiple of a and b can be written as $\frac{ab}{cd}$

   $\therefore$ $a|\frac{ab}{cd}$, $b|\frac{ab}{cd}$

   $\therefore$ cd|b, cd|a

   $\because$ gcd(a,b) = c

   $\therefore$ d = 1

   $\therefore$ lcm(a,b)= $\frac{ab}{cd}$=$\frac{ab}{c}$=$\frac{ab}{\text{gcd}(a,b)}$

   $\therefore$ gcd(a,b)*lcm(a,b)=a*b

7. $\because$ For the integer $a_0a_1a_2...a_{n-1}$,

   $a_0a_1a_2...a_{n-1}$ mod 9=a_0*10^{n-1}+a_1*10^{n-2}+...a_{n-1}*10^0 mod 9

   =a_0+a_1+...a_{n-1} mod 9

   $\therefore$ $a_0a_1a_2...a_{n-1}$ mod 9 = a_0+a_1+...a_{n-1} mod 9

8. (a) $\frac{p+1}{2p}$

   (b) $\because$ $(x+p)^2$ mod p = x^2+2px+p^2 mod p = x^2 mod p

   $\therefore$ 只须讨论$0 \le x \le p-1$时 x^2 mod p 的值

   $\therefore$ 只须证明$0 \le x \le p-1$时 x^2 mod p 的不同值的数量为$\frac{p+1}{2p}$

   $\because$ x^2 mod p = $(-x)^2$ mod p

$= p^2+2p(-x)+(-x)^2 \bmod p$

$=(p-x)^2 \bmod p$

$\therefore\ 0 \le x \le p-1$时 $x^2 \bmod p$ 的不同值的数量$\le \frac{p+1}{2p}$

$\therefore$ 只须证明$0 \le x \le \frac{p-1}{2p}$时 $x^2 \bmod p$ 的值互不相同

设$0 \le x_1 < x_2 \le \frac{p-1}{2p}$，则

$(x_2^2 - x_1^2)\ \bmod p =$

$(x_2 + x_1)(x_2 - x_1) \bmod p$

$\because\ (x_2 + x_1) < p, (x_2 - x_1) < p$

$\therefore\ (x_2 + x_1)(x_2 - x_1) \bmod p \ne 0$

$\therefore\ x_1^2 \bmod p \ne x_2^2 \bmod p$

$\therefore$ 命题成立

9. (a) (1) Reflexive: ∵For every element a, a = a (mod p)

(2) Symmetric: ∵For every element a, b and a = b(mod p). → b = a(mod p)

(3) Transitive: ∵For every element a, b, c and a = b(mod p). b = c(mod p) → a = c(mod p)

(b)Addition:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Multiplication:

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1