Homework 5

Sun Kai

5110309061

1. (mod 11) 80035

= 835\*1035\*1035

= 835\*(-1)35\*(-1)35

=835

=8\*82\*832

=8\*9\*916

=6\*48

=6\*54

=6\*32

=10

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

i = k\*p + a (kN). Then i (mod p) equals a.

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

1. ∵x-y=5

∴3x-3y=1

∵3x+2y=1

∴5y=0

∴y=0

∴x=5, y=0

1. (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.

1. ∵ 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)

∴400-1=167 (mod 997)

1. gcd(a,b)\*lcm(a,b)=a\*b

Proof: Let c = gcd(a,b)

∴ c|a, c|b

∴ a|, b|

∴ is the common multiple of a and b

So the least common multiple of a and b can be written as

∴ a|, b|

∴ cd|b, cd|a

∵ gcd(a,b) = c

∴ d = 1

∴ lcm(a,b)===

∴ gcd(a,b)\*lcm(a,b)=a\*b

1. ∵ For the integer a0a1a2…an-1,

a0a1a2…an-1 mod 9=a0\*10n-1+a1\*10n-2+…an-1\*100 mod 9

=a0+a1+…an-1 mod 9

∴ a0a1a2…an-1 mod 9 = a0+a1+…an-1 mod 9

1. (a)

(b) ∵ (x+p)2 mod p = x2+2px+p2 mod p = x2 mod p

∴ 只须讨论时x2 mod p的值

∴ 只须证明时x2 mod p的不同值的数量为

∵ x2 mod p = (-x)2 mod p

= p2+2p(-x)+(-x)2 mod p

=(p-x)2 mod p

∴ 时x2 mod p的不同值的数量

∴ 只须证明时x2 mod p的值互不相同

设，则

mod p =

mod p

∵

∴ mod p 0

∴ mod p mod p

∴ 命题成立

1. (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 |