Homework TWO

潘亦晟
515021910384

March 23, 2018

Problem 1.

Solution 1) Determine whether 227 and 79 are relatively prime.

$$227 = 79 \times 2 + 69$$

$$79 = 69 \times 1 + 10$$

$$69 = 10 \times 6 + 9$$

$$10 = 9 \times 1 + 1$$

Thus,

$$gcd(227, 69) = 1$$

They are relatively prime.

(2) Determine whether 22337 and 17241 are relatively prime.

$$22337 = 17241 \times 1 + 5096$$

$$17241 = 5096 \times 3 + 1953$$

$$5096 = 1953 \times 2 + 1190$$

$$1953 = 1190 \times 1 + 763$$

$$1190 = 763 \times 1 + 427$$

$$763 = 427 \times 1 + 336$$

$$427 = 336 \times 1 + 91$$

$$336 = 91 \times 3 + 63$$

$$91 = 63 \times 1 + 28$$

$$63 = 28 \times 2 + 7$$

$$28 = 7 \times 4$$

Thus

$$gcd(22337, 17241) = 7$$

Problem 2.

Solution 1) Find the multiplicative inverse of 4565 and 15447.

$$15447 = 4565 \times 3 + 1752 \rightarrow 1 = 15447 \times 1863 - 6304 \times 4565$$

$$4565 = 1752 \times 2 + 1061 \rightarrow 1 = 1752 \times 1863 - 4565 \times 715$$

$$1752 = 1061 \times 1 + 691 \rightarrow 1 = 1752 \times 433 - 1061 \times 715$$

$$1061 = 691 \times 1 + 370 \rightarrow 1 = 691 \times 433 - 1061 \times 282$$

$$691 = 370 \times 1 + 321 \rightarrow 1 = 691 \times 151 - 370 \times 282$$

$$370 = 321 \times 1 + 49 \rightarrow 1 = 321 \times 151 - 370 \times 131$$

$$321 = 49 \times 6 + 27 \rightarrow 1 = 321 \times 20 - 49 \times 131$$

$$49 = 27 \times 2 + 22 \rightarrow 1 = 27 \times 20 - 49 \times 11$$

$$27 = 22 \times 1 + 5 \rightarrow 1 = 27 \times 9 - 22 \times 11$$

$$22 = 5 * 4 + 2 \rightarrow 1 = 5 \times 9 - 22 \times 2$$

$$5 = 2 \times 2 + 1 \rightarrow 1 = 5 \times 1 - 2 \times 2$$

Thus the multiplicate inverse of 4565 and 15447 is

$$15447 - 6304 = 9143$$

(2) 7932 and 11458 don't have the multiplicative inverse because 7932 and 11458 are both even,so not relatively prime.

Problem 3.

Solution

$$\phi(105) = \phi(7 \times 5 \times 3) = (1 - \frac{1}{7})(1 - \frac{1}{5})(1 - \frac{1}{3}) = 6 \times 4 \times 2 = 48$$

Problem 4.

Solution 1)Using Euler's generalization, we can get

$$\phi(21) = 12$$

$$227^{5496213} \mod 21 = 227^{12 \times 4583017 + 9} \mod 21 = 227^{9} \mod 21$$

(2) Euler's Theorem :

$$a^{\phi(n)} \equiv 1 \mod n$$

If n is prime , $\phi(n) = n - 1$,so we can get the Fermat's little theorem:

$$a^{n-1} \equiv 1 \mod n$$

Problem 5.

Solution 1)

$$17^{27} \quad mod \quad 23 = 17^{16} \times 17^8 \times 17^2 \times 17^1 \quad mod \quad 23$$

$$17^2 \quad mod \quad 23 \equiv 13 \quad mod \quad 23$$

$$17^4 \quad mod \quad 23 \equiv 13^2 \quad mod \quad 23 \equiv 8 \quad mod \quad 23$$

$$17^8 \quad mod \quad 23 \equiv 8^2 \quad mod \quad 23 \equiv 18 \quad mod \quad 23$$

$$17^{16} \quad mod \quad 21 \equiv 18^2 \quad mod \quad 23 \equiv 2 \quad mod \quad 23$$

Thus,

$$17^{23} \equiv (2 \times 18 \times 13 \times 17) \quad mod \quad 23 = 21$$

(2)

$$65535_{10} = 1111111111111111_2$$

$$65537_{10} = 10000000000000000_2$$

We need to calculate modular multiplication (15+15) = 30 times for a^{65535}*and*16+1=17*timesfor*a^{65537}. Therefore, calculate a^{65535} will be more expensive.

Problem 6.

Solution 1)$\mathbb{Z}_{11}/0$ and $\mathbb{Z}_{79}/0$ are multiplicative group since 11 and 79 are prime.

(2)$\mathbb{Q}$ can't form a multiplicative group because the element 0 doesn't have an inverse.

Problem 7.

Solution 1. $(\mathbb{Z}_5, +)$ is a cyclic group with a generator of $g = 1$;

2. $(\mathbb{Z}_8^*, *)$ isn't a cyclic group;

3. $(\mathbb{Z}_1 3^*, *)$ is a cyclic gruop with a generator of $g = 11$.