MEM204-Number Theory

16th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 27/05/2020

University of Crete

Answers of the 6th set

Exercise 1

Exercise

Show that if a is primitive modulo n, then a^k is primitive modulo n if and only if $(\varphi(n), k) = 1$. Moreover, if $\mathbb{Z}_n$ contains one primitive root, it contains a total of $\varphi(\varphi(n))$ primitive roots, given by the above rule.

Exercise 1

We have that a is primitive, i.e., $\text{ord}(a) = |\mathbb{Z}_n^*| = \varphi(n)$. Further, a^k is primitive if and only if

$$\text{ord}(a^k) = \varphi(n) \iff \frac{\text{ord}(a)}{\gcd(k, \text{ord}(a))} = \varphi(n)$$

$$\overset{\text{ord}(a)=\varphi(n)}{\iff} \gcd(k, \varphi(n)) = 1.$$

Next, notice that

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{a^k \mid 1 \leq k \leq \varphi(n)\} = \mathbb{Z}_n^*.$$

Combining the above, yields that identifying the primitive elements of $\mathbb{Z}_n^*$, is equivalent to identifying the exponents $1 \leq k \leq \varphi(n)$ that are co-prime to $\varphi(n)$. By the definition of the φ-function, the number of these exponents is $\varphi(\varphi(n))$.

Exercise 2

Exercise

Find all the primitive roots modulo 54 *and modulo* 55*.*

Exercise 2

We begin with 55. Since $55 = 5 \cdot 11$, we conclude is not of the forms 2, 4, p^r or $2p^r$, thus there are no primitive roots modulo 55.

Next, notice that $54 = 2 \cdot 3^3$, hence there are primitive roots modulo 54. First, we will find a special primitive root modulo 54 and then, based on this, using Exercise 1, build the whole set of primitive roots modulo 54.

The possible orders of the elements of $\mathbb{Z}_{54}^*$ are the divisors of $\varphi(54) = 18$, hence $1, 2, 3, 6, 9$ and 18. We explicitly check the elements one-by-one, until we find one whose order is not $1, 2, 3, 6$ or 9:

Exercise 2

$$1^1 \equiv 1 \pmod{54} \Rightarrow \operatorname{ord}(\bar{1}) = 1$$

$$5^1 \equiv 5 \pmod{54},\ 5^2 \equiv 25 \pmod{54},\ 5^3 \equiv 17 \pmod{54},$$
$$5^6 \equiv 19 \pmod{54},\ 5^9 \equiv 53 \pmod{54} \Rightarrow \operatorname{ord}(\bar{5}) = 18.$$

It follows that 5 is a primitive root modulo 54. By Exercise 1, there are exactly

$$\varphi(\varphi(54)) = \varphi(18) = 6$$

such roots. More precisely, the numbers in the interval $1 \leq k \leq \varphi(54) = 18$, that are co-prime to 18 are

$$1, 5, 7, 11, 13, 17,$$

hence, the distinct primitive roots modulo 54 are the numbers

$$5, 5^5, 5^7, 5^{11}, 5^{13}, 5^{17}.$$

Exercise 3

Exercise

Prove that if one knows n and $\varphi(n)$ and knows that $n = pq$ for some distinct primes p and q, then he/she can compute p and q without performing any hard computation, such as the factorization of n.

Exercise 3

We have that

$$\varphi(n) = (p-1)(q-1) = n-p-q+1 \Rightarrow p+q = A = n-\varphi(n)+1.$$

In particular, the number $p+q$ is easily computed as a linear expression of known numbers. Moreover,

$$n = pq = p(A-p) \Rightarrow p^2 - Ap + n = 0,$$

that is, p can be easily computed as a root of a quadratic equation. One can easily verify that q is the other root of the same equation.

Exercise 9

Exercise

Prove that the following equations have integer solutions.

1. $102x + 165y = 3$.
2. $4x^2 + 211y = 5$.

Exercise 9

1. Here, we have that $\gcd(102, 165) = 3 \mid 3$, hence the equation is solvable.
2. This equation is solvable if and only if $211 \mid 5 - 4x^2$, for some x (in which case y will be the quotient of this division). This is equivalent to the solvability of the congruence

$$4x^2 \equiv 5 \pmod{211} \overset{4^{-1} \equiv 53 \pmod{211}}{\iff} x^2 \equiv 54 \pmod{211}.$$

The above is solvable iff 54 is a quadratic residue modulo 211, that is, iff $\left(\frac{54}{211}\right) = 1$, which we can computationally verify.

Exercise 10

Exercise

Show that the only integer solution of $x^2 + y^2 = 3z^2$ is the trivial one.

Answer

Legendre's theorem implies that if $x^2 + y^2 - 3z^2 = 0$ has a non-trivial solution, then -1 is a quadratic residue modulo 3, a contradiction.

Exercise 11

Exercise

Find all the integer solutions of the equation

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = m,$$

where $x, y, z, m \in \mathbb{Z}$*,* $x, y, z \neq 0$ *and* x, y, z *are pairwise co-prime.*

Exercise 11

The equation is equivalent to

$$x^2z + y^2x + z^2y = mxyz.$$

Let p be a prime divisor of x. The above equation implies that $p \mid z^2y$, that is $p \mid y$ or $p \mid z$. However, both possibilities contradict to the fact that x, y, z are pairwise co-prime. Thus x has no prime divisors that is $x = \pm 1$.

Similarly, $y, z = \pm 1$. It follows that the solutions of the original equation are:

$$(x, y, z, m) = (1, 1, 1, 3), (1, 1, -1, -1), (1, -1, 1, -1), (1, -1, -1, -1),$$
$$(-1, 1, 1, -1), (-1, 1, -1, -1), (-1, -1, 1, -1), (-1, -1, -1, 3).$$

Exercise 12

Exercise

Show that there does not exist any integer n, such that $\frac{7n-1}{4}, \frac{5n+3}{12} \in \mathbb{Z}$.

Answer

Assume that such integer exists. Then $7n - 1 = 4k$ and $5n + 3 = 12\ell$, for some $k, \ell \in \mathbb{Z}$. We then have that

$$\begin{cases} 7n - 1 = 4k \\ 5n + 3 = 12\ell \end{cases} \Rightarrow \begin{cases} 35n = 20k + 5 \\ 35n = 84\ell - 21 \end{cases} \Rightarrow 84\ell - 20k = 26.$$

However, the latter is not solvable, since $(84, 20) = 4 \nmid 26$, and we reach a contradiction.

Exercise 13

Exercise

Find all the right triangles, with integer sides, whose area equals their perimeter.

Exercise 13

Clearly, we are looking for all the Pythagorian triples (a, b, c), such that $ab/2 = a + b + c$. From the characterization of these triples, it follows that we are looking for the triples (d, u, v), such that $\gcd(u, v) = 1$, $0 < v < u$, not both of u, v are odd, $d > 0$ and

$$\frac{(d2uv)d(u^2 - v^2)}{2} = (2duv) + d(u^2 - v^2) + d(u^2 + v^2).$$

The above is equivalent to

$$dv(u - v) = 2.$$

Exercise 13

Since d, v and $u - v$ are positive integers, it follows that,

$$\begin{cases} d = 1, \\ v = 1, \\ u = 3, \end{cases} \quad \text{or} \quad \begin{cases} d = 1, \\ v = 2, \\ u = 3, \end{cases} \quad \text{or} \quad \begin{cases} d = 2, \\ v = 1, \\ u = 2. \end{cases}$$

In the first case though, both u, v are odd, so we accept only the second and the third cases. It follows that the only right triangles with the above specifications are the ones with sides $5, 12, 13$ or $6, 8, 10$.

Exercise 14

Exercise

Examine whether the equation $75x^2 + 27y^2 - 30z^2 = 0$ *has a non-trivial integer solution.*

Exercise 14

Notice that once we divide by 3, the equation becomes

$$(5x)^2 + (3y)^2 - 10z^2 = 0.$$

Set $X = 5x$, $Y = 3y$ and $Z = z$. Now the equation becomes

$$X^2 + Y^2 - 10Z^2 = 0. \tag{1}$$

Notice that we can apply Legendre's theorem in (1). By doing so, we get that we do, in fact, have an integer solution $(X, Y, Z) \neq (0, 0, 0)$ of (1). It follows that we have a non-trivial rational solution $\left(\frac{X}{5}, \frac{Y}{3}, Z\right)$ of the original equation. Finally, from this we get that $(3X, 5Y, 15Z)$ is a non-trivial integer solution of the original equation.

Good luck with the exams

ENJOY THE SUMMER!