UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
NUMBER THEORY - MEM204 (SPRING SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

6th exercise set - Answers

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

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

$$\mathrm{ord}(a^k) = \phi(n) \iff \frac{\mathrm{ord}(a)}{\gcd(k, \mathrm{ord}(a))} = \phi(n) \overset{\mathrm{ord}(a)=\phi(n)}{\iff} \gcd(k, \phi(n)) = 1.$$

Next, notice that

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

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

**Exercise 2.** Find all the primitive roots modulo $54$ and modulo $55$.

*Answer.* 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 $\phi(54) = 18$, 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 $9$:

$$\begin{aligned}
&1^1 \equiv 1 \pmod{54} \Rightarrow \mathrm{ord}(\bar{1}) = 1 \\
&5^1 \equiv 5 \pmod{54},\ 5^2 \equiv 25 \pmod{54},\ 5^3 \equiv 17 \pmod{54}, \\
&\qquad\qquad 5^6 \equiv 19 \pmod{54},\ 5^9 \equiv 53 \pmod{54} \Rightarrow \mathrm{ord}(\bar{5}) = 18.
\end{aligned}$$

It follows that $5$ is a primitive root modulo $54$.

By Exercise 1, there are exactly

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

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

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

hence, the distinct primitive roots modulo 54 are the numbers

$$5, 5^5, 5^7, 5^{11}, 5^{13}, 5^{17}. \qquad \square$$

**Exercise 3.** Prove that if one knows $n$ and $\phi(n)$ 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 $n$.

*Answer.* We have that

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

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. $\square$

**Exercise 4.** Find all the integer solutions of $2x^3 + xy - 7 = 0$.

*Answer.* Clearly, $x \neq 0$, hence the above can be rewritten as

$$y = \frac{-2x^3 + 7}{x}.$$

Hence, the rational solutions are of the form $(x, (-2x^3+7)/x)$, where $x \in \mathbb{Q} \setminus \{0\}$. It follows that the integer solutions are those where $x \in \mathbb{Z} \setminus \{0\}$ and $x \mid (-2x^3 + 7)$. The latter is true if and only if $x \mid 7$. It follows that the integer solutions are $(1, 5)$, $(-1, -9)$, $(7, -97)$ and $(-7, -99)$. $\square$

**Exercise 5.** Find all the integer solutions of $15x^2 - 7y^2 = 9$.

*Answer.* Let $(x, y)$ be an integer solution of the above. Then

$$-7y^2 \equiv 9 \pmod 5 \ \Rightarrow \ y^2 \equiv 3 \pmod 5.$$

However, the latter is impossible, since $\left(\frac{3}{5}\right) = -1$. It follows that there are no integer solutions of this equation. $\square$

**Exercise 6.** Find all the integer solutions of $221x + 340y = 51$.

*Answer.* First, we employ the Euclidean algorithm and (from its first part) we get $(221, 340) = 17$. Since $17 \mid 51$, we know that the equation has integer solutions.

Next, from the second part of the Euclidean algorithm, we find that

$$17 = 2 \cdot 340 - 3 \cdot 221.$$

We multiply the above equation by 3 (because $51/17 = 3$) and get:

$$51 = 221(-9) + 340 \cdot 6,$$

in other words, $(-9, 6)$ is a solution. It follows that all the solutions are

$$x = -9 + 20t, \ y = 6 - 13t, \ t \in \mathbb{Z}. \qquad \square$$

**Exercise 7.** Find all the integer solutions of $6x + 4y + 8z = 2$.

*Answer.* First, notice that $(6, 4, 8) = 2 \mid 2$, hence the equation has integer solutions. Then, set $w = 3x + 2y$ (in general, we take the co-prime parts of the coefficients of $x$ and $y$, so, here, we have $(6, 4) = 2$ and we take $3 = 6/2$ and $2 = 4/2$ respectively). Now, the original equation becomes

$$2w + 8z = 2.$$

By using the method for two-variable linear Diophantine equations described earlier, we find that all the solutions of the above are given by

$$w = 5 + 4t,\ z = -1 - t,\ t \in \mathbb{Z}.$$

Now, it remains to solve

$$3x + 2y = 5 + 4t.$$

Again, the two-variable method yields the solutions

$$x = (5 + 4t) + 2s,\ y = -(5 + 4t) - 3s,\ s \in \mathbb{Z}.$$

It follows that the whole set of solutions of the original equation are given by

$$x = 5 + 4t + 2s,\ y = -5 - 4t - 3s,\ z = -1 - t,\ s, t \in \mathbb{Z}. \qquad \square$$

**Exercise 8.** Does the equation

$$9x^2 + 35y^2 - 721z^2 = 0 \tag{1}$$

have non-trivial solutions?

*Answer.* First, we notice that Legendre's theorem cannot be directly applied to (1), as (i) the coefficients are not square-free and (ii) the coefficients are not pairwise co-prime. However, we can tranform it into one that meets Legendre's theorem criteria.

Namely, we multiply everything by the appearing gcd's (here 7) and gather all the resulting and pre-existing squares and we get the equivalent equation

$$7(3x)^2 + 5(7y)^2 - 103(7z)^2 = 0.$$

We set $X = 3x, Y = 7y$ and $Z = 7z$ and get

$$7X^2 + 5Y^2 - 103Z^2 = 0. \tag{2}$$

In the above equation, we can apply Legendre's theorem.

By computing the corresponding Legendre symbols, we can easily check that, in fact, the numbers $-5 \cdot 7$, $103 \cdot 5$ and $103 \cdot 7$ are quadratic residues modulo $103$, $7$ and $5$ respectively, so the existence of an integer solution of (2) is ensured.

Let $(u, v, w)$ be this solution. It follows that $\left(\frac{u}{3}, \frac{v}{7}, \frac{z}{7}\right)$ is a (rational) solution of (1) and that $(7u, 3v, 3z)$ is an integer solution of (1). $\square$

**Exercise 9.** Prove that the following equations have integer solutions.

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

*Answer.* 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.** 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.** 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.

*Answer.* 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:

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

**Exercise 12.** 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.** Find all the right triangles, with integer sides, whose area equals their perimeter.

*Answer.* 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

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

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

*Answer.* 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

$$X^2 + Y^2 - 10Z^2 = 0. \tag{3}$$

Notice that we can apply Legendre's theorem in (3). By doing so, we get that we do, in fact, have an integer solution $(X, Y, Z) \neq (0, 0, 0)$ of (3). 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. □