MEM204-Number Theory

10th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 06/05/2020

University of Crete

Primitive roots

Introduction

Recall that, if $(a, n) = 1$, the order (τάξη) of a modulo n is defined as the smallest positive exponent x, such that

$$a^x \equiv 1 \pmod{n},$$

and it is denoted by $\mathrm{ord}_n(a)$. Further, we have seen that $\mathrm{ord}_n(a) \mid \varphi(n)$. Today, we will study the elements with order $\varphi(n)$.

Definition

Let a and $n > 1$ be such that $(a, n) = 1$. Then a is called a primitive root modulo n (πρωταρχική ρίζα modulo n) if $\mathrm{ord}_n(a) = \varphi(n)$.

A natural question is whether primitive roots modulo n exist and, if yes, how many of them are there?

Remark

For the remaining lecture, we will assume that $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$ and $(a, n) = 1$.

Some basics

Proposition

The integer a is a primitive root modulo n iff $\{1, a, a^2, \dots, a^{\varphi(n)-1}\}$ is a reduced set of representatives modulo n.

Proof.

Let a be primitive $\pmod n$. Then $1, a, a^2, \dots, a^{\varphi(n)-1}$ are distinct $\pmod n$ (why?). Hence, they form a subset of $\mathbb{Z}_n^*$ of cardinality $\varphi(n)$ and the result follows.

Conversely, assume that $\{1, a, a^2, \dots, a^{\varphi(n)-1}\}$ is a reduced set of representatives $\pmod n$. Then $a^{\varphi(n)} \equiv 1 \pmod n$, while $a^d \not\equiv 1 \pmod n$ for all $1 \leq d < \varphi(n)$. The result follows. $\square$

Powers of 2

Proposition

If $n = 2^m$, $m \geq 3$, then $a^{\varphi(n)/2} \equiv 1 \pmod{n}$.

Proof.

We will use induction on m. Since $(a, n) = 1$, a is odd, i.e. $a = 2b + 1$ for some b. Now, for $m = 3$ we have:

$$a^{\varphi(n)/2} \equiv (2b+1)^2 \equiv 4b(b+1) + 1 \equiv 1 \pmod{8},$$

since $b(b+1)$ is even for every b.

Next, assume that $a^{\varphi(2^k)/2} \equiv 1 \pmod{2^k} \iff a^{2^{k-2}} = 2^k t + 1$, for some t. Finally, we have

$$a^{\varphi(2^{k+1})/2} \equiv (a^{2^{k-2}})^2 \equiv 2^{2k}t^2 + 2^{k+1}t + 1 \equiv 1 \pmod{2^{k+1}}. \quad \square$$

The above, combined with the facts that 1 is a primitive root modulo 2 and that 3 is a primitive root modulo 4, yield the following.

Proposition

There are primitive roots modulo 2^m if and only if $m = 1$ or 2.

Another non-existence result

Proposition

Let $n = rs$, with $(r, s) = 1$ and $r, s > 2$. Then $a^{\varphi(n)/2} \equiv 1 \pmod{n}$.

Proof.

Since $(a, r) = 1$, we have that $a^{\varphi(r)} \equiv 1 \pmod{r}$. The facts that r and s are co-prime and that φ is multiplicative yield $\varphi(n) = \varphi(r)\varphi(s)$. It follows that

$$a^{\varphi(n)/2} \equiv (a^{\varphi(r)})^{\varphi(s)/2} \equiv 1 \pmod{r}.$$

Similarly, we get $a^{\varphi(n)/2} \equiv 1 \pmod{s}$ and the result follows from the Chinese Remainder Theorem. □

Corollary

Let $n = rs$, with $(r,s) = 1$ and $r,s > 2$. Then there are no primitive roots modulo n.

The non-existence results we have seen so far cover all the numbers, except

$$2, 4, p^r, 2p^r,$$

where p is an odd prime and $r \geq 1$.

Our next step is to prove that in these cases, the existence of primitive roots is ensured.

An auxiliary lemma (from Group Theory)

Lemma

Let $k \geq 1$. *Then* $\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{\gcd(\mathrm{ord}_n(a), k)}$.

Proof.

Set $r = \mathrm{ord}_n(a)$ and $d = \gcd(r, k)$. Then $r = df$ and $k = de$, for some co-prime numbers e and f. Thus

$$(a^k)^f \equiv a^{er} \equiv (a^r)^e \equiv 1 \pmod{n}.$$

Further, $m \geq 1$ is such that $(a^k)^m \equiv 1 \pmod{n}$, iff $r \mid km$, that is, iff $f \mid me$. Since $(f, e) = 1$ the latter is equivalent to $f \mid m$ and the result follows. □

Odd primes

Proposition

Let p be an odd prime and $d \mid p-1$. Then there are exactly $\varphi(d)$ elements of $\mathbb{Z}_p$ of order d.

Proof.

Presented in the next slides. □

Corollary

Let p be an odd prime. There are exactly $\varphi(p-1)$ primitive roots modulo p.

Proof of the proposition

Let $\psi(d)$ be the number of elements of $\mathbb{Z}_p$ with order d. Suppose that $\psi(d) \neq 0$. We will show that, in that case, $\psi(d) = \varphi(d)$. Since $\psi(d) \neq 0$, there exists some a, such that $\text{ord}_p(a) = d$. This means that the numbers $1, a, \ldots, a^{d-1}$ are non-congruent modulo p. Moreover, these numbers satisfy

$$x^d - 1 \equiv 0 \pmod{p},$$

which has at most d solutions modulo p. In other words, they are exactly the solutions of the above congruence. It follows that the elements of $\mathbb{Z}_p$ of order d are found among them. From the last lemma, we get that $\text{ord}_p(a^k) = \text{ord}_p(a)/\gcd(\text{ord}_p(a), k)$, that is $\text{ord}_p(a^k) = d \iff (k, d) = 1$. The result follows from the fact that there are exactly $\varphi(d)$ exponents with this property.

Proof of the proposition

Moreover, by definition, one gets $\sum_{d|p-1} \psi(d) = p - 1$. We also have that $\sum_{d|p-1} \varphi(d) = p - 1$, that is,

$$\sum_{d|p-1} \psi(d) = \sum_{d|p-1} \varphi(d),$$

which combined with the fact that, for every $d \mid p - 1$, $\psi(d) \leq \varphi(d)$, yields

$$\psi(d) = \varphi(d),$$

for every $d \mid p - 1$. The proof is now complete.

A related open problem and active research

Although, the results we saw earlier, not only ensure the existence of primitive roots modulo p, for every prime p, but also imply the number of such roots, we do not yet have an effective (in computer terms) way of finding one such root, when p is large.

A problem that has recently started attracting attention, is the construction of *almost* primitive roots (i.e., high-order elements).

p^r and $2p^r$ where p is an odd prime

Proposition

Let p be an odd prime and let $r \geq 1$. Then there are primitive roots modulo p^r and $2p^r$.

We will first prove the above for p^r and then, based on this, for $2p^r$.

Proof of the case $n = p^r$

Let a be a primitive root $\pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$, i.e., $a^{p-1} = 1 + yp$, for some y. First, we will show that there exists some $b \equiv a \pmod{p}$, such that

$$b^{p^{j-1}(p-1)} = 1 + p^j z_j, \text{ where } p \nmid z_j,$$

for all $j \geq 1$. We will use induction on j.

For $j = 1$, Let $b = a + px$. Then

$$b^{p-1} = (a + px)^{p-1} = 1 + py + \sum_{k=1}^{p-2} \binom{p-1}{k} a^k (px)^{p-1-k}.$$

Hence, $b^{p-1} = 1 + pz_1$, where $z_1 \equiv y + (p-1)a^{p-2}x \pmod{p}$. Since $p \nmid (p-1)a^{p-2}$, we may choose x, such that $p \nmid z_1$ and the result follows.

Next, assume that the statement holds for $j = m$. Then for $j = m + 1$, we get

$$b^{p^m(p-1)} \overset{I.H.}{=} (1 + p^m z_m)^p = \sum_{k=0}^{p} \binom{p}{k} (p^m z_m)^k = 1 + p^{m+1} z_{m+1},$$

where

$$z_{m+1} = z_m + \sum_{k=2}^{p} z_m^k p^{m(k-1)-1}.$$

Since $p \nmid z_m$, but p divides every other term of the above sum, we obtain $p \nmid z_{m+1}$. The induction is now complete.

Set $d = \mathrm{ord}_{p^r}(b)$. Then $d \mid \varphi(p^r) = p^{r-1}(p-1)$. Moreover, b is primitive modulo p and $b^d \equiv 1 \pmod{p}$, hence $p - 1 \mid d$, that is, $d = (p-1)c$ for some c, hence $(p-1)c \mid p^{r-1}(p-1)$, i.e., $c \mid p^{r-1}$, hence $c = p^s$, for $s \leq r - 1$, i.e., $d = (p-1)p^s$.

Proof of the case $n = p^r$

Our proof will be complete once we show that, above, $s = r - 1$. The induction argument proved that

$$b^{p^s(p-1)} = 1 + p^{s+1} z_{s+1}, \text{ where } p \nmid z_{s+1}.$$

Since $\mathrm{ord}_{p^r}(b) = (p-1)p^s$,

$$b^{p^s(p-1)} = 1 + p^r z,$$

for some z. So, if $s < r - 1$, we obtain $p \mid z_{s+1}$, a contradiction.

The case $n = p^r$ is now settled.

Proof of the case $n = 2p^r$

We continue with the case $n = 2p^r$. Let b be a primitive root $\pmod{p^r}$. Then $b + p^r$ is also primitive $\pmod{p^r}$ and (since p^r is odd) one of these numbers is odd. Let g be the odd number among them. Then $(g, 2p^r) = 1$. Set $d = \mathrm{ord}_{2p^r}(g) = d$. Then, clearly, $d \mid \varphi(2p^r) = \varphi(p^r)$.

Moreover, $g^d \equiv 1 \pmod{p^r}$ and $\mathrm{ord}_{p^r}(g) = \varphi(p^r)$, that is, $\varphi(p^r) \mid d$. It follows that $d = \varphi(p^r) = \varphi(2p^r)$, that is, g is primitive $\pmod{2p^r}$.

Cardinality of primitive roots

Proposition

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.

Proof.

Exercise □

Synopsis

To sum up, in this lecture we proved the following.

Theorem

Let $n > 1$. Then there exist primitive roots modulo n if and only if

$$n = 2, 4, p^m, 2p^m,$$

where p is an odd prime and $m \geq 1$. In this case, there exist exactly $\varphi(\varphi(n))$ primitive roots modulo n and if a is one of them, the other are congruent (modulo n) to a^k, for some $1 \leq k \leq \varphi(n)$, with $(k, \varphi(n)) = 1$.

Stay home, stay safe!