

# Primitive Existentialism by Root Counting

Stefanus<sup>1</sup>

<sup>1</sup> Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: September 2, 2017)

## Abstract

Proving the existence of primitive roots modulo  $2, 4, p, p^\alpha$  and  $2p^\alpha$  and the non existence of any other modulus by explicitly counting the number of roots of the polynomial  $x^d - 1 \equiv 0$  where  $d|\varphi(n)$ .

**\* Parental Advisory, Explicit Content \***

In the following discussion we will derive the number of primitive roots modulo  $n$  (not necessarily prime) **Explicitly!** and in doing so we will prove that only  $2, 4, p, p^\alpha$  and  $2p^\alpha$  have primitive roots.

**Basic Ingredients**

To achieve our goal of counting primitive roots we need the following well known facts.

- First, any polynomial of degree  $f$  defined on a field has at most  $f$  roots, see ent.pdf Proposition 2.5.3.
- Next, the fact that  $\mathbb{Z}/p\mathbb{Z}$  is a field as shown in Exercise 2.12 of ent.pdf.
- Chinese Remainder Theorem and its useful cousin Chinese Remainder Map.
- Lastly using an application of Proposition 2.5.5 of ent.pdf which states that for each divisor  $d|(p-1)$ , the polynomial of degree  $d$  has exactly  $d$  roots in  $\mathbb{Z}/p\mathbb{Z}$ .
- And of course all other good stuffs from elementary number theory, like the Euler Totient function  $\varphi(n)$ , Fermat's Little Theorem, order of an element of  $\mathbb{Z}/n\mathbb{Z}$ , etc.

Although Proposition 2.5.5 can be automatically extended to  $d|\varphi(n)$  with  $n$  not prime as long as  $\mathbb{Z}/n\mathbb{Z}$  forms a field, the problem is that for  $n$  not prime  $\mathbb{Z}/n\mathbb{Z}$  is guaranteed not to be a field. So for now we just concentrate on  $n$  being prime.

**Counting Primal Roots**

With all these in mind we proceed to calculate the number of primitive roots in the unit group  $(\mathbb{Z}/n\mathbb{Z})^*$ . Fermat's Little Theorem tells us that every number in the unit group  $(\mathbb{Z}/n\mathbb{Z})^*$  satisfy the following  $x^{\varphi(n)} \equiv 1 \pmod{n}$ , therefore the polynomial  $x^{\varphi(n)} - 1 \equiv 0 \pmod{n}$  has exactly  $\varphi(n)$  roots since that's the number of elements in the unit group.

To find the primitive roots we want to find elements of the unit groups that are **not** roots of  $x^d - 1 \equiv 0$  where  $d|\varphi(n)$  because these roots indicate that their order is less than  $\varphi(n)$ .

Now suppose that  $\varphi(n)$  is just a product of two primes

$$\varphi(n) = q_1 q_2$$

From the  $q_1 q_2$  roots of  $x^{\varphi(n)} \equiv 1$ , how many of them are roots of  $x^{q_1} \equiv 1$  and how many are roots of  $x^{q_2} \equiv 1$ ? The roots that are not covered by  $x^{q_1} \equiv 1$  and  $x^{q_2} \equiv 1$  will be the primitive roots of  $n$ . So are there any?

From the  $q_1 q_2$  roots of  $x^{\varphi(n)} \equiv 1$  we need to subtract  $q_1$  roots that belong to  $x^{q_1} \equiv 1$  and  $q_2$  roots that belong to  $x^{q_2} \equiv 1$ , this is because we know that there are exactly  $q_1$  and  $q_2$  roots for those two polynomials as given by Proposition 2.5.5 of ent.pdf.

But in doing the subtractions we were double counting because 1 is always a root of  $x^d - 1 \equiv 0$  whatever  $d$  is, so when subtracting the roots of  $x^{q_1} \equiv 1$  we already remove 1, thus we need to add 1 back, the number of primitive roots are then

$$\begin{aligned} q_1 q_2 - q_1 - q_2 + 1 &= (q_1 - 1)(q_2 - 1) \\ &= \varphi(q_1 q_2) \\ &= \varphi(\varphi(n)) \end{aligned}$$

Now what happens if  $\varphi(n)$  has three distinct prime factors? We do the same, we start with  $q_1 q_2 q_3$  as the total number of roots, we then remove the ones already covered by  $q_1 q_2$ , followed by  $q_1 q_3$  and finally  $q_2 q_3$ . But in doing so we are again over counting because while removing the roots of  $x^{q_1 q_2} \equiv 1$  we already removed the roots of  $x^{q_1} \equiv 1$  (and of  $x^{q_2} \equiv 1$ ) but when we removed the roots of  $x^{q_1 q_3} \equiv 1$  we again remove the roots of  $x^{q_1} \equiv 1$ , so we need to add them back in.

$$q_1 q_2 q_3 - q_1 q_2 - q_1 q_3 - q_2 q_3 + q_1 + q_2 + q_3$$

But as we are removing and adding back over counted roots, we also remove and add 1 (since 1 is always a root), here we removed it three times and then we added it back in three times, but 1 still should be removed, so the final tally is

$$\begin{aligned} q_1 q_2 q_3 - q_1 q_2 - q_1 q_3 - q_2 q_3 + q_1 + q_2 + q_3 - 1 &= (q_1 - 1)(q_2 - 1)(q_3 - 1) \\ &= \varphi(\varphi(n)) \end{aligned}$$

and the pattern continues. But what if we have a more generic

$$\varphi(n) = q_1^{a_1} q_2^{a_2} \dots q_n^{a_n}$$

The pattern is still the same, let's limit  $n = 3$  to see a concrete example, again we start with  $q_1^{a_1} q_2^{a_2} q_3^{a_3}$  we then remove the roots belonging to  $q_1^{a_1} q_2^{a_2} q_3^{a_3-1}$  followed by the ones in  $q_1^{a_1} q_2^{a_2-1} q_3^{a_3}$  and finally  $q_1^{a_1-1} q_2^{a_2} q_3^{a_3}$ .

Note that by removing the roots of  $q_1^{a_1} q_2^{a_2} q_3^{a_3-1}$  we are already removing the roots of all its divisors. But just like before, we are over counting because we removed the roots of  $q_1^{a_1} q_2^{a_2-1} q_3^{a_3-1}$  twice, once from  $q_1^{a_1} q_2^{a_2} q_3^{a_3-1}$  and another time from  $q_1^{a_1} q_2^{a_2-1} q_3^{a_3}$ , so we need to add them back in

$$\begin{aligned} & q_1^{a_1} q_2^{a_2} q_3^{a_3} - q_1^{a_1} q_2^{a_2} q_3^{a_3-1} - q_1^{a_1} q_2^{a_2-1} q_3^{a_3} - q_1^{a_1-1} q_2^{a_2} q_3^{a_3} \\ & + q_1^{a_1} q_2^{a_2-1} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3} \end{aligned}$$

but again, here we've removed the roots of  $q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3-1}$  three times and then added them back in three times, but we know that they should be removed, so the final tally is

$$\begin{aligned} & q_1^{a_1} q_2^{a_2} q_3^{a_3} - q_1^{a_1} q_2^{a_2} q_3^{a_3-1} - q_1^{a_1} q_2^{a_2-1} q_3^{a_3} - q_1^{a_1-1} q_2^{a_2} q_3^{a_3} \\ & + q_1^{a_1} q_2^{a_2-1} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3} \\ & - q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3-1} \end{aligned}$$

which is just  $(q_1^{a_1} - q_1^{a_1-1})(q_2^{a_2} - q_2^{a_2-1})(q_3^{a_3} - q_3^{a_3-1}) = \varphi(q_1^{a_1} q_2^{a_2} q_3^{a_3}) = \varphi(\varphi(n))$ . Note that we don't need to mess with other divisors of  $\varphi(n)$  because for example the roots of  $x^s - 1$  are already covered by the roots of  $x^t - 1$  as long as  $s|t$ .

So the generic strategy is to start with  $\varphi(n)$  roots, express  $\varphi(n)$  in terms of its primal constituents and then start removing the roots of the next highest divisor of  $\varphi(n)$  and then take care of all the double counting until there's no more over counting and stop. This pattern persists for a generic prime  $n$ .

Since  $\varphi(\varphi(n))$  can never be zero and as long as  $n$  is prime, we have also not only proven that there are always primitive roots modulo a prime  $p$  but also how many there are.

The key here is of course that the polynomial  $x^d - 1 \equiv 0$  has *exactly*  $d$  roots, and this rests on the ring  $\mathbb{Z}/n\mathbb{Z}$  being a field, what happens if it's not a field?

## **Composite Conundrum**

First we tackle the case of  $n = p^\alpha$ . Here  $\varphi(n) = p^{\alpha-1}(p-1)$  and we tackle the problem of  $x^d - 1 \equiv 0 \pmod{p^\alpha}$  with  $d|\varphi(n)$  in three steps, first, when  $d|p^{\alpha-1}$ , second  $d|(p-1)$  and lastly the combination of both.

The goal here is to show that  $x^d - 1 \equiv 0 \pmod{p^\alpha}$  has exactly  $d$  roots if  $d|\varphi(p^\alpha)$ . First case is  $d = p^\beta$ ,  $\beta < \alpha$ .

### **First Case**, $d|p^{\alpha-1}$

The motivation for this is as follows, take for example  $p^\alpha = 3^2$ ,  $\varphi(3^2) = 3 \cdot 2$ , and  $d = 3$ . If we cube each element of  $\mathbb{Z}/3^2\mathbb{Z} = \{1, 2, 3, \dots, 3^2 = 9\}$  we get

$$\{1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3\} \equiv \{1, 8, 0, 1, 8, 0, 1, 8, 0\} \pmod{3^2}$$

So it looks like any number  $a = 1 + x \cdot (3^2/3)$  will have  $a^3 = \{1 + x \cdot (3^2/3)\}^3 \equiv 1 \pmod{3^2}$ , and the generic formula when  $d = p^\beta$ ,  $\beta \leq \alpha - 1$  seems to be  $a = 1 + x \cdot p^{\alpha-\beta}$ . Exponentiating to the  $d^{\text{th}}$  power we get

$$(1 + x \cdot p^{\alpha-\beta})^{p^\beta} = 1 + \sum_{j=1}^{p^\beta} \binom{p^\beta}{j} (x \cdot p^{\alpha-\beta})^j$$

We want to show that the sum is  $\equiv 0 \pmod{p^\alpha}$ .

### **Binomial Bifurcation**

Before we tackle the sum above, we will bifurcate our discussion into properties of binomial coefficients.

**Proposition E.0.** (“E” here stands for Explicit :) First, for  $j \geq 1$

$$\binom{p^n}{j} = \begin{cases} k \cdot p^n & \text{if } \gcd(j, p^n) = 1 \\ l \cdot p^{n-w} & \text{if } \gcd(j, p^n) = p^w, 1 \leq w \leq n \end{cases}$$

where  $\gcd(k, p) = \gcd(l, p) = 1$ .

*Proof.* Let's rewrite the binomial as

$$\begin{aligned} \binom{p^n}{j} &= \frac{p^n!}{j!(p^n - j)!} \\ &= \frac{p^n \cdot (p^n - 1) \cdots (p^n - j + 1)}{j \cdot (j - 1) \cdots 1} \end{aligned}$$

Note that the goal here is to count the number of  $p$  in the binomial coefficient.

One thing to note is that the numerator and denominator have the same number of terms. Now let  $r$  be the highest exponent such that  $p^r \leq j$  and rearrange the fraction as

$$\frac{1}{j} \cdot \frac{1}{(j-1)} \cdots \left(\frac{p^n}{p^r}\right) \cdots \left(\frac{p^n - p}{p^r - p}\right) \cdots \left(\frac{p^n - 2p}{p^r - 2p}\right) \cdots \left(\frac{p^n - (p^{r-1} - 1)p}{p}\right) \cdots$$

$$\cdots \frac{p^n - p^r + 1}{1} \cdot \frac{(p^n - p^r)^*}{1} \cdots \frac{p^n - j + 1}{1}$$

The terms in brackets are the only terms in the numerator (and denominator) that contain  $p$ , so basically we align the terms in the numerator and denominator so that those who contain  $p$  are grouped together, and the last bracket with  $()^*$  on it indicates that the numerator contains  $p$  while the denominator doesn't, note that this term doesn't exist if  $j = p^r$  since the binomial stops one term earlier, let's see this with a concrete example, take  $p^n = 5^2$  and  $j = 7$ , we then get

$$\frac{1}{7} \frac{1}{6} \left(\frac{25}{5}\right) \frac{24}{4} \frac{23}{3} \frac{22}{2} \frac{21}{1} \frac{(20)^*}{1}$$

and if  $j = 5^1$  we get

$$\left(\frac{25}{5}\right) \frac{24}{4} \frac{23}{3} \frac{22}{2} \frac{21}{1}$$

the term with  $()^*$  doesn't exist in this case.

The reason behind this rearrangement is that we want to count the number of  $p$  in the fraction, by grouping the terms in the numerator and denominator that contain  $p$  we reduce the problem into analyzing those terms only. These terms are of the form  $(p^n - yp)/(p^r - yp)$  if  $(y, p^n) = p^{t-1}$  we can express  $yp = xp^t$  with  $(x, p) = 1$  and

$$\frac{p^n - xp^t}{p^r - xp^t} = \frac{p^{n-t} - x}{p^{r-t} - x}$$

now the numerator and denominator no longer have any factor of  $p$  since  $x$  is co-prime to  $p$ , thus the only terms in brackets that contain  $p$  are

$$\left(\frac{p^n}{p^r}\right) \quad \text{and} \quad \frac{(p^n - p^r)^*}{1}$$

thus the binomial coefficient is just  $k \cdot p^n$  since

$$\left(\frac{p^n}{p^r}\right) \cdot \frac{(p^n - p^r)}{1} = \frac{p^n(p^{n-r} - 1)}{1}$$

and  $\gcd(p, p^{n-r} - 1) = 1$ . Now if  $j = p^r$  then we don't have the  $()^*$  term, the binomial stops one term earlier, thus the binomial is equal to  $l \cdot p^{n-r}$ .

**Proposition E.1.** For an odd prime  $p$  and  $m, n > 0$  we have

$$(1 + xp^m)^{p^n} \equiv 1 + xp^{m+n} \pmod{p^{m+n+1}}$$

*Proof.* First we expand

$$(1 + xp^m)^{p^n} = 1 + \sum_{j=1}^{p^n} \binom{p^n}{j} (xp^m)^j$$

From Proposition E.0 we know that

$$\binom{p^n}{j} (xp^m)^j = \begin{cases} k \cdot x^j p^{n+jm} & \text{if } \gcd(j, p^n) = 1 \\ l \cdot x^{yp^r} p^{n-r+mypr} & \text{if } \gcd(j, p^n) = p^r \rightarrow j = yp^r, \gcd(y, p) = 1, r > 0 \end{cases}$$

For the first case  $n + jm > n + m$  if  $j > 1$  and for the second case  $mypr > r$  for any  $y$  and  $r$  thus

$$\binom{p^n}{j} (xp^m)^j = \begin{cases} x \cdot p^{n+m} & \text{if } j = 1 \\ v \cdot p^{n+m+1} & \text{if } j > 1 \end{cases}$$

therefore

$$\begin{aligned} (1 + xp^m)^{p^n} &= 1 + xp^{n+m} + vp^{n+m+1} \\ &\equiv 1 + xp^{n+m} \pmod{p^{n+m+1}} \end{aligned}$$

Going back to our proposed solution  $(1 + x \cdot p^{\alpha-\beta})^{p^\beta}$ , utilizing Proposition E.1 with  $m = \alpha - \beta$  and  $n = \beta$  we get

$$\begin{aligned} (1 + x \cdot p^{\alpha-\beta})^{p^\beta} &= 1 + x \cdot p^{\alpha-\beta+\beta} + v \cdot p^{\alpha-\beta+\beta+1} \\ &= 1 \pmod{p^\alpha} \end{aligned}$$

The question now is how many of these numbers  $(1 + x \cdot p^{\alpha-\beta})$  incongruent modulo  $p^\alpha$  there are, this is equivalent to the number of unique values for  $x$ . The obvious answer is  $0 \leq x < p^\beta$ , meaning we have  $p^\beta$  solutions for  $x^{p^\beta} - 1 \equiv 0$ .

Are there more than that? What if we found a number  $a^{p^\beta} - 1 \equiv 0$  besides the above? say there's the case then

$$a^{p^\beta} \equiv 1 \pmod{p^\alpha} \rightarrow a^{p^\beta} \equiv 1 \pmod{p}$$

but by Fermat's Little Theorem this is forbidden because this means that either  $p^\beta | (p-1)$  or  $(p-1) | p^\beta$ , except for  $a \equiv 1 \pmod{p}$ . So the only other possible roots is in the form  $1 + xp$ .

To prove that such roots do not exist we again use Proposition E.1, we start with

$$(1 + x' \cdot p^{\alpha-\beta-1})^{p^\beta} = 1 + x'p^{\alpha-1} + vp^\alpha$$

we want the RHS to be  $\equiv 1 \pmod{p^\alpha}$  thus

$$\begin{aligned} 1 + x'p^{\alpha-1} + vp^\alpha &= 1 + wp^\alpha \\ x' &= p(w - v) \\ p &| x' \end{aligned}$$

but this means that the necessary condition for  $(1 + x' \cdot p^{\alpha-\beta-1})^{p^\beta} \equiv 1 \pmod{p^\alpha}$  is that  $p|x'$ . We now repeat the process with

$$(1 + x'' \cdot p^{\alpha-\beta-2})^{p^\beta} = 1 + x''p^{\alpha-2} + v'p^{\alpha-1}$$

and we still want the RHS to be  $\equiv 1 \pmod{p^\alpha}$  therefore

$$\begin{aligned} 1 + x''p^{\alpha-2} + v'p^{\alpha-1} &= 1 + w'p^\alpha \\ x'' &= p(pw' - v') \\ p &| x'' \end{aligned}$$

so the necessary condition is still that  $p|x''$  but this means that the solution is of the form  $1 + x' \cdot p^{\alpha-\beta-1}$  but even in this case  $p|x'$  so the solution is just  $1 + x \cdot p^{\alpha-\beta}$ , we can keep repeating with  $p^{\alpha-\beta-3}$  and so on until we reach  $p^1$  and working back up we will see that the solution must be of the form  $1 + x \cdot p^{\alpha-\beta}$ . So we have shown that  $x^{p^\beta} - 1 \equiv 0$  has exactly  $p^\beta$  solutions.

### **Second Case, $d|(p-1)$**

Next case is when  $d|(p-1)$ , this one is a bit trickier and we need to utilize induction. By Proposition 2.5.5 of ent.pdf we know that  $x^d - 1 \equiv 0 \pmod{p}$  has exactly  $d$  solutions, the problem we have now is that  $\mathbb{Z}/p^\alpha\mathbb{Z}$  is no longer a field. But we can build the proof one power at a time.



Base case is  $x^d - 1 \equiv 0 \pmod{p}$ , based on this how can we find the solutions to  $x^d - 1 \equiv 0 \pmod{p^2}$ ? Well, we know that if there is a solution, say  $a^d \equiv 1 \pmod{p^2}$ , then  $a$  has to also satisfy

$$a^d \equiv 1 \pmod{p}$$

meaning  $a$  is also a root  $\pmod{p}$ , *i.e.* it is of the form  $a + np$ , our task is to see whether we can find such  $n$  to get a solution  $\pmod{p^2}$ , (existence of  $a \pmod{p}$  is already guaranteed by Proposition 2.5.5). Let's see how this works

$$\begin{aligned} (a + np)^d &= a^d + da^{d-1}np + p^2t, & a^d &= 1 + mp \\ &\equiv 1 + mp + da^{d-1}np \pmod{p^2} \end{aligned}$$

$a^d = 1 + mp$  since  $a^d \equiv 1 \pmod{p}$ . We want this whole thing to be  $1 \pmod{p^2}$  so

$$\begin{aligned} 1 + mp + da^{d-1}np &\equiv 1 \pmod{p^2} \\ \rightarrow mp + da^{d-1}np &\equiv 0 \pmod{p^2} \\ da^{d-1}np &\equiv -mp \pmod{p^2} \\ n &\equiv -m(da^{d-1})^{-1} \pmod{p} \end{aligned}$$

the inverse is guaranteed since  $da^{d-1}$  is co-prime to  $p$  (this is a crux of the proof as we shall see soon) and  $\mathbb{Z}/p\mathbb{Z}$  is a field since  $p$  is prime, so  $n$  is guaranteed to exist (modulo  $p$ ). So we have the following solutions

$$a + (n + sp)p, \quad s \geq 0$$

however, for  $s \geq 1$ ,  $a + np + sp^2$  is bigger than  $p^2$ , so we only have one such  $a + np < p^2$  (note that  $n < p$ ). So for every root  $a^d \equiv 1 \pmod{p}$  we have a *unique* root  $a^d \equiv 1 \pmod{p^2}$ . Using this info we can prove a unique root  $\pmod{p^3}$ , but this time we substitute  $a = 1 + mp^2$  instead of  $a = 1 + mp$ , and in this way the induction goes.

The uniqueness part is crucial because we want to show that there are exactly  $d$  roots and since we prove that there is a unique  $a$  we are done.

### **Non-existence of Primitive Roots modulo $2^\alpha$ , $\alpha \geq 3$**

The proofs above give us an idea on how to prove that  $2^\alpha$  with  $\alpha \geq 3$  doesn't have primitive roots. Say we elevate the roots of  $x^2 \equiv 1 \pmod{4}$  to modulo 8 just like before,

we will get 4 roots, 1, 3, 5, 7, but  $x^4 \equiv 1 \pmod{8}$  only has 4 roots and they are already covered by  $x^2 \equiv 1$ , that means that there are no primitive roots. Again, taking 1, 3, 5, 7, and elevating them to 9, 11, 13, 15, these eight are the roots of  $x^4 \equiv 1 \pmod{16}$  and they are also all the roots of  $x^8 \equiv 1 \pmod{16}$  so 16 has no primitive roots and so on. Let's see this in detail.

**Proposition E.2.** Any number  $1 + 2c$  with  $0 \leq c < 2^{\alpha-1}$  are all roots of  $x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$ , so there are  $2^{\alpha-1}$  roots and these roots are also roots of  $x^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$ , this is true for  $\alpha \geq 3$ .

*Proof.* We will use induction, base case is 8, with  $a = 1, 3, 5, 7$  and from the assumption we know that  $a^2 \equiv 1 \pmod{8} = 1 + 8m$  and so going from mod 8  $\rightarrow$  16,

$$\begin{aligned} a^2 &= 1 + 8m \\ a^4 &= (1 + 8m)^2 \\ &= 1 + 16m + 64m^2 \\ &\equiv 1 \pmod{16} \end{aligned}$$

we now extend the solutions mod 8 from 1, 3, 5, 7 to 9, 11, 13, 15, so basically  $a \rightarrow a + 8$ , going to mod 16 we get

$$\begin{aligned} (a + 8)^2 &= a^2 + 16a + 64 & a^2 &= 1 + 8m \\ &\rightarrow \equiv 1 + 8m \pmod{16} \end{aligned}$$

and so  $(a + 8)^4 \equiv 1 \pmod{16}$  as well. We can thus repeat the inductive process to complete the proof which is a straightforward process by replacing 8 with  $2^n$  and 16 with  $2^{n+1}$  and therefore omitted here :)

In short, the roots of  $x^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$  must satisfy  $x^{\varphi(2^\alpha)} \equiv 1 \pmod{2}$ , which means that  $x$  must be an odd number. However, we have shown above that all odd numbers  $< 2^\alpha$  are roots of  $x^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ , thus we have covered all possible roots of  $x^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$  with the roots of  $x^{\varphi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$ .

**Proposition E.3.** As a direct consequence of Proposition E.2,  $2^\alpha$  with  $\alpha > 2$  has no primitive roots :)

This also shows why there is primitive root modulo 4, because in this case  $\varphi(4)/2 = 1$  and  $x^1 \equiv 1$  can only have one root and not two.

**Last Case**,  $d|p^{\alpha-1}(p-1)$

The last case we have is a combination of the above two,  $d|p^{\alpha-1}(p-1)$ , the proof is therefore also a combination of the two :) Let's denote  $d = xy$  with  $x|p^{\alpha-1} \rightarrow x = p^\beta$  with  $\beta < \alpha$  and  $y|(p-1)$  and by virtue of  $(p, p-1) = 1$  we have  $(x, y) = 1$  as well.

To tackle this we first find the solutions for  $a^y - 1 \equiv 0 \pmod{p^{\alpha-\beta}}$  where  $y|(p-1)$ . But this is exactly the same as our previous case, the roots are the same as  $a^y - 1 \equiv 0 \pmod{p}$  elevated to  $\pmod{p^{\alpha-\beta}}$  by the induction method above.

After finding all roots of  $a^y - 1 \equiv 0 \pmod{p^{\alpha-\beta}}$ , we then use these roots and extend them

$$\begin{aligned} (a + w \cdot p^{\alpha-\beta})^{xy} &= (a + w \cdot p^{\alpha-\beta})^{p^\beta y} \\ &= (a^y)^{p^\beta} + \sum_{j=1}^{p^\beta} \binom{p^\beta}{j} (w \cdot p^{\alpha-\beta})^j \\ &= (1 + s \cdot p^{\alpha-\beta})^{p^\beta} + \sum_{j=1}^{p^\beta} \binom{p^\beta}{j} (w \cdot p^{\alpha-\beta})^j \\ &= 1 + \sum_{i=1}^{p^\beta} \binom{p^\beta}{i} (s \cdot p^{\alpha-\beta})^i + \sum_{j=1}^{p^\beta} \binom{p^\beta}{j} (w \cdot p^{\alpha-\beta})^j \end{aligned}$$

just like before, using Proposition E.1, the sums are 0  $\pmod{p^\alpha}$ , the challenge now is to show that there are no other roots other than the ones shown above. Suppose there is another root,  $b$ , then

$$\begin{aligned} b^{xy} &= \left(b^{p^\beta}\right)^y \equiv 1 \pmod{p^\alpha} \\ \rightarrow \left(b^{p^\beta}\right)^y &\equiv 1 \pmod{p^{\alpha-\beta}} \end{aligned}$$

but when extending the roots  $a^y \equiv 1 \pmod{p}$  to  $\pmod{p^{\alpha-\beta}}$  the extension is unique  $\pmod{p^{\alpha-\beta}}$ , so if there's another root it must be of the form  $a + w \cdot p^{\alpha-\beta}$  hence there can't be any other roots.

**The Case of  $2p^\alpha$**

For  $2p^\alpha$  we can repeat the whole process again (although we have to first show that there are unique roots modulo  $2p$  and then extend it to  $\pmod{2p^\alpha}$ , this will be discussed later) or we can just utilize the following fact

**Proposition E.4.** If the order of  $x$  modulo  $a$  is  $o_a$  and the order of  $x \bmod b$  is  $o_b$  and  $\gcd(a, b) = 1$  then the order of  $x \bmod ab$  is  $\text{lcm}(o_a, o_b)$ .

*Proof.* First suppose we pick a number  $x$  and two other numbers  $a, b$  with  $\gcd(m, n) = 1$ , the orders of  $x$  are given by

$$x^{o_a} \equiv 1 \pmod{a}$$

$$x^{o_b} \equiv 1 \pmod{b}$$

Denote  $\text{lcm}(o_a, o_b) = d$ , it is then true that

$$x^d \equiv 1 \pmod{a}$$

$$= 1 + au$$

$$x^d \equiv 1 \pmod{b}$$

$$= 1 + bv$$

Furthermore

$$x^d = x^d$$

$$1 + au = 1 + bv$$

$$au = bv$$

Since  $\gcd(a, b) = 1$  this means that  $b|u$  and  $a|v \rightarrow au = bv = abs$ , thus

$$x^d = 1 + abs$$

$$\equiv 1 \pmod{ab}$$

We know that the order of  $x$  modulo  $ab$  must be divisible by  $o_a$  and  $o_b$  and  $d = \text{lcm}(o_a, o_b)$  is the smallest number that is divisible by  $o_a$  and  $o_b$ , therefore  $x^d \equiv 1 \pmod{ab}$  means that the order of  $x$  modulo  $ab$  is indeed  $d = \text{lcm}(o_a, o_b)$ .

Since we have proven that there are primitive roots,  $g$ , modulo  $p^\alpha$ , using Proposition E.4, the order of  $g$  modulo  $2p^\alpha$  is then given by  $\text{lcm}(\varphi(2), \varphi(p^\alpha)) = \varphi(p^\alpha) = \varphi(2p^\alpha)$ , thus the primitive roots modulo  $p^\alpha$  are also primitive roots modulo  $2p^\alpha$  and there are as many primitive roots for both as  $\varphi(2p^\alpha) = \varphi(p^\alpha)$ .

TABLE I

$w = \prod_1^z$	$p_1^{n_1}$	$p_2^{n_2}$	$p_3^{n_3}$ $\dots$ $p_z^{n_z}$
$\varphi(p_i^{n_i}) =$	$p_1^{n_1-1}(p_1 - 1)$	$p_2^{n_2-1}(p_2 - 1)$	$p_3^{n_3-1}(p_3 - 1)$ $\dots$ $p_z^{n_z-1}(p_z - 1)$
	$x^{a_1} \equiv 1 \pmod{p_1^{n_1}}$	$x^{a_2} \equiv 1 \pmod{p_2^{n_2}}$	$x^{a_3} \equiv 1 \pmod{p_3^{n_3}}$ $\dots$ $x^{a_z} \equiv 1 \pmod{p_z^{n_z}}$
	$a_1   (p_1^{n_1-1}(p_1 - 1))$	$a_2   (p_2^{n_2-1}(p_2 - 1))$	$a_3   (p_3^{n_3-1}(p_3 - 1))$ $\dots$ $a_z   (p_z^{n_z-1}(p_z - 1))$

### All Other Cases

We now use this result to characterize the primitive roots of a number  $w$  based on its prime factorization. Thanks to Euclid, every number  $w$  can be factorized into

$$\begin{aligned}
w &= p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots p_z^{n_z} \\
&= \prod_{i=1}^z p_i^{n_i} \\
\rightarrow \varphi(w) &= \prod_{i=1}^z p_i^{n_i-1} (p_i - 1)
\end{aligned}$$

We now list every number  $1 < x < w$  for each distinct  $\pmod{p_i^{n_i}}$ , where  $a_i$  is the order of each  $x$  modulo  $p_i^{n_i}$  where each  $a_i$  is limited by Euler's theorem to be  $a_i | (p_i^{n_i-1}(p_i - 1))$ , see Table. I As shown above, the order of  $x$  modulo  $w$  is given by

$$x^{\text{lcm}(a_1, a_2, \dots, a_z)} \equiv 1 \pmod{p_1^{n_1} p_2^{n_2} \dots p_z^{n_z}}$$

since  $\gcd(p_i^{n_i}, p_j^{n_j}) = 1$  for any  $i, j$ . For  $x$  to be a primitive root of  $w$  we need

$$\text{lcm}(a_1, a_2, \dots, a_z) = p_1^{n_1-1}(p_1 - 1) p_2^{n_2-1}(p_2 - 1) \dots p_z^{n_z-1}(p_z - 1)$$

Now since each  $a_i | (p_i^{n_i-1}(p_i - 1))$ , for the above requirement to hold it has to be that each  $a_i = (p_i^{n_i-1}(p_i - 1))$ . However,  $2 | (p_i - 1)$  for every  $p_i \neq 2$ , therefore

$$\text{lcm}(a_1, a_2, \dots, a_z) \leq p_1^{n_1-1}(p_1 - 1) p_2^{n_2-1}(p_2 - 1) \dots p_z^{n_z-1}(p_z - 1)$$

Thus except for  $2, 4, p^\alpha$  and  $2p^\alpha$ , there is no primitive roots since the lcm is always smaller than  $\varphi(w)$ .

### Conclusion

We have shown a method to prove the existence of primitive roots by counting their exact number through simple root counting of  $x^\varphi(p) \equiv 1$  defined on  $\mathbb{Z}/p\mathbb{Z}$ , primitive roots are therefore the roots of aforementioned polynomial that are not roots of  $x^d \equiv 1 \pmod{p}$  where  $d|\varphi(p)$ , special cases must be handled for odd primes  $p^\alpha$  and  $2^\alpha$ , other cases can be derived from these. The conclusion is that only numbers of the form  $2, 4, p, p^\alpha, 2p^\alpha$  have primitive roots.

### Some Afterthoughts

The key ingredient here is of course the fact that a polynomial of degree  $f$  over a field has only at most  $f$  roots. Why doesn't it work for other cases? For one thing, if  $\mathbb{Z}/n\mathbb{Z}$  is not a field, it implies that  $n$  is composite. Take for example  $x^2 \equiv 1 \pmod{15}$ , there are actually four roots because the roots correspond to the Chinese Remainder map (see Shoup's book), they are

$$x \equiv \pm 1 \pmod{3}$$

$$x \equiv \pm 1 \pmod{5}$$

What happens if we restrict our polynomial to the unit group,  $(\mathbb{Z}/n\mathbb{Z})^*$ , instead? Well, for one thing the unit group doesn't have 0, so we can't set our polynomial to 0, fine, let's append 0 to the unit group, will that work? Using the same example above, it will still not work because 1 is obviously co-prime to 3 and 5 and 15, thus the four  $x$ 's will still be co-prime to 15 and they are all roots.

So any odd composite number won't work, how about special cases like  $p^\alpha$ ? Using our extension mechanism above we can show that a polynomial over  $\mathbb{Z}/p^\alpha\mathbb{Z}$ . Say we have a root  $a$  on a polynomial of degree  $f$  modulo  $p$

$$\sum_{i=0}^f c_i x^i, \quad c_f \not\equiv 0$$

Let's do it one term at a time ( $j > 0$ )

$$\begin{aligned} (a + np)^j &= a^j + \sum_{k=1}^j \binom{j}{k} a^{j-k} (np)^k \\ &\equiv a^j + ja^{j-1}np \pmod{p^2} \end{aligned}$$

so

$$\begin{aligned}
\sum_{i=0}^f c_i a^i &= \sum_{i=0}^f c_i (a^i + i a^{i-1} n p) \pmod{p^2} \\
&= \sum_{i=0}^f c_i a^i + \sum_{i=1}^f c_i i a^{i-1} n p \pmod{p^2} \\
&= w p + \sum_{i=1}^f c_i i a^{i-1} n p \pmod{p^2}
\end{aligned}$$

we want the whole thing to be  $\equiv 0 \pmod{p^2}$

$$\begin{aligned}
w p + \sum_{i=1}^f c_i i a^{i-1} n p &\equiv 0 \pmod{p^2} \\
\sum_{i=1}^f c_i i a^{i-1} n &\equiv -w \pmod{p} \\
n \cdot s &\equiv -w \pmod{p} \quad s = \sum_{i=1}^f c_i i a^{i-1}
\end{aligned}$$

Note that this is also true going from  $\text{mod } p^n$  to  $p^{n+1}$ , as we will cancel  $p^n$  from both sides instead of  $p$  in the last step above. There are a few things to consider

- If  $p|w$  but  $p \nmid s$  then  $n|p$ , in this case the root modulo  $p^2$ ,  $a'$ , is the same as the one modulo  $p$ ,  $a$  because then  $a' = a + p^2 t$  and we want  $a' < p^2$ .
- If  $p \nmid w$  but  $p \nmid s$  then there is a unique  $n$  and therefore there is only one root modulo  $p^2$  corresponding to a root modulo  $p$ .
- If  $p \nmid w$  but  $p|s$  then there is no solution for  $n$  but this only means that there are less roots modulo  $p^2$  compared to those of modulo  $p$ .
- If  $p|w$  but  $p|s$  then  $n$  can be anything but that also means that any  $a' = a + n p$  will be a root modulo  $p^2$ , this means that there are  $p$  new roots  $a'$  associated with the root  $a \pmod{p}$ .

So as long as  $p \nmid w$  or  $p \nmid s$  we are good but looking closely,  $s$  is just the derivative of the polynomial, so

**Proposition E.5.** For a polynomial of degree  $f$  over a ring  $\mathbb{Z}/p^\alpha\mathbb{Z}$ , there are at most  $f$  roots as long as the derivative of that polynomial has no roots other than zero mod  $p$  or the roots modulo  $p$  are not roots modulo  $p^2$ .

And for our case  $x^d - 1 \equiv 0$ , the derivative is just  $dx^{d-1} \equiv 0$  and so the derivative is only zero if  $x \equiv 0$  and thankfully that cannot be the case so using this method we could've proven the case of  $p^\alpha$  rather quickly.

### Extending Roots from $p$ to $2p$

So how do we extend the roots of  $x^d \equiv 1 \pmod{p}$  to modulo  $2p$ ? Well, for one thing if we have roots  $x^d \equiv 1 \pmod{2p}$  then it is also true that each root satisfies

$$\begin{aligned} x^d &\equiv 1 \pmod{2} \\ x^d &\equiv 1 \pmod{p} \end{aligned}$$

from the first congruence it is guaranteed to be odd and from the second congruence the root mod  $2p$  must also be a root modulo  $p$ . Say  $a$  is a root modulo  $p$  so by default  $a < p$ . If  $a$  is even the root modulo  $2p$  must then be of the form  $a + p$  because, one it has to be odd and two it must be less than  $2p$ . If  $a$  is already odd then  $a$  is also a root modulo  $2p$ .

The important question now is whether  $a$  is also a root of  $x^d \equiv 1 \pmod{2p}$ , just because  $a^d$  satisfy the above two congruences does it mean that  $a^d \equiv 1 \pmod{2p}$ ? The answer is yes as it is guaranteed by the Chinese Remainder Map.

Here's how it works. Say we have a system of congruences (for simplicity assume there are only 2)

$$\begin{aligned} y &\equiv c_1 \pmod{p_1} \\ y &\equiv c_2 \pmod{p_2} \end{aligned}$$

Chinese Remainder Theorem guarantees that there is such a unique  $y \equiv c \pmod{p_1 p_2}$ . Let's exponentiate  $y \rightarrow y^u \equiv c^u \pmod{p_1 p_2}$ , then the congruences we have above become

$$\begin{aligned} y^u &\equiv c_1^u \pmod{p_1} \\ y^u &\equiv c_2^u \pmod{p_2} \end{aligned}$$



but again, Chinese Remainder Theorem guarantees that solving  $c_1^u \pmod{p_1}$  and  $c_2^u \pmod{p_2}$  generates a unique solution modulo  $p_1 p_2$ . Therefore this solution must be the same as  $c^u$  since expressing  $c^u$  in terms of  $\pmod{p_1}$  and  $\pmod{p_2}$  generate the same exact congruences. This is called the Chinese Remainder Map, see Shoup's book for more details. But we are not done, for our case of  $x^d \equiv 1 \pmod{2p}$  we have to show  $c^u \equiv 1 \pmod{2p}$ , lucky for us,  $c_1^u \equiv 1 \pmod{2}$  and  $c_2^u \equiv 1 \pmod{p}$  and we know that if we have a system of congruences

$$\begin{aligned} x &\equiv k \pmod{h_1} \\ x &\equiv k \pmod{h_2} \\ &\vdots \\ x &\equiv k \pmod{h_m} \end{aligned}$$

then  $x$  is given by  $x \equiv k \pmod{h_1 h_2 \cdots h_m}$ . Therefore  $c^u \equiv 1 \pmod{2p}$  and Chinese Remainder Map guarantees that the solution mod  $p$  is also a solution mod  $2p$ .

Therefore the roots of  $x^d \equiv 1 \pmod{2p}$  are given by

$$x = \begin{cases} a & \text{if } a \text{ is odd} \\ a + p & \text{if } a \text{ is even} \end{cases}$$

where  $a$  is a root of  $x^d \equiv 1 \pmod{p}$  and  $a < p$ . What this means is that every root modulo  $p$  is mapped uniquely to a root modulo  $2p$ . Can there be any other roots? No because any root modulo  $2p$  must be a root modulo  $p$  and we have shown above that the extension to mod  $2p$  is unique.

The awesome thing about the Chinese Remainder Map is that it works not only for multiplication (exponentiation is just a repeated multiplications) but also for addition (well, multiplication is just repeated additions). Therefore, if we have a polynomial of order  $f$ ,  $P_f(x)$  modulo  $p$  and  $a$  is a root mod  $p$  then by the construction above we can extend it to mod  $2p$ , but instead of  $1 \pmod{2}$  we get  $c_0 \pmod{2}$  for the condition where  $c_0$  is the coefficient of  $x^0$  in  $P_f(x)$

$$x = \begin{cases} a & \text{if } a \text{ has the same parity as } -c_0 \\ a + p & \text{if } a \text{ has the opposite parity of } -c_0 \end{cases}$$

Because we extend the roots mod  $p$  to mod  $2p$  uniquely, just like Proposition E.5, we have

**Proposition E.5.1** as long as the derivative doesn't have a root other than 0 modulo  $p$  or the roots mod  $p$  are not root modulo  $p^2$ , a polynomial of degree  $f$  modulo  $2p^\alpha$  has at most  $f$  roots.

Why doesn't it work for  $2^\beta p^\alpha$ ? For mod  $2^\beta p^\alpha$ , we can have more roots than the degree of the polynomial, this is because we can extend the roots from  $2p \rightarrow 4p \rightarrow \dots$ . Once we have the roots mod  $2p$ , we just need to add  $2p$  to this root to get another root, and it is also a root, again, guaranteed by the Chinese Remainder Map, say we have a root,  $a + p$ , mod  $2p$  we set up the following system of congruences

$$x \equiv a + p + 2p \pmod{4}$$

$$x \equiv a + p + 2p \pmod{p}$$

which gives us  $x = a + p + 2p$  as a solution modulo  $4p$  since it is less than  $4p$ , putting this into the polynomial we get

$$P_f(x) - c_0 \equiv -c_0 \pmod{4}$$

$$P_f(x) - c_0 \equiv -c_0 \pmod{p}$$

and by the Chinese Remainder Map as explained above it must be a solution modulo  $4p$ .

Let's see it with a concrete example,  $x^2 \equiv 1 \pmod{3}$ . Extending it from  $3 \rightarrow 2 \cdot 3$ , we see that the roots mod 3 are 1 and 2. Here,  $c_0$  is odd, so  $1 \rightarrow 1$  and  $2 \rightarrow 2 + 3 = 5$  and the roots mod  $2 \cdot 3$  are 1 and 5. If we now go from  $2 \cdot 3 \rightarrow 4 \cdot 3$ , we just need to add  $2 \cdot 3$  to 1 and 5, so the roots mod  $4 \cdot 3$  are 1, 5, 7, 11, they are all roots because they satisfy the congruences mod  $p$  and mod 4 and by the help of our Chinese friend they are also roots mod  $4p$ .

**Proposition E.6.** We can use this as a generic strategy to find roots of polynomial over a generic ring  $\mathbb{Z}/n\mathbb{Z}$ , write  $n$  in terms of its primal constituents

$$n = 2^\beta \prod_m q_m^{\alpha_m}$$

and then we find the roots over each *odd* prime ring,  $\mathbb{Z}/q_m\mathbb{Z}$ , we extend the roots from  $q \rightarrow q^\alpha$  for each  $q$ , once we have all this we just use Chinese Remainder Theorem to get

the combined solution modulo  $\prod_m q_m^{\alpha_m}$ . If we have a factor of  $2^\beta$  we then extend the roots to modulo  $2 \prod_m q_m^{\alpha_m}$  by sufficiently adding  $\prod_m q_m^{\alpha_m}$  depending on the parity of  $-c_0$ , once we've done this we add more roots by adding  $2 \prod_m q_m^{\alpha_m}$  followed by adding  $2^2 \prod_m q_m^{\alpha_m}$  and so on until we add  $2^{\beta-1} \prod_m q_m^{\alpha_m}$ .

So if there are  $k$  roots modulo  $\prod_m q_m^{\alpha_m}$  there will be  $2^{\beta-1}k$  roots modulo  $2 \prod_m q_m^{\alpha_m}$ .