Primitive Existentialism in Counting Roots

Stefanus[1]

[1] Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: August 29, 2017)

Abstract

Proving the existence of primitive roots modulo 2,4, p and $2p^\alpha$ by explicit counting the number of roots of the polynomial $x^d - 1 \equiv 0$.

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 and $2p^\alpha$ have primitive roots.

Basic Ingredients

We will achieve our goal of counting roots using a few 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.

- 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 $\mathbb{Z}/p\mathbb{Z}$

Although Proposition 2.5.5 can be automatically extended to $d|\varphi(n)$ when n is 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 $(\mathbb{Z}/n\mathbb{Z})^*$. As in above we know the polynomial $x^{\varphi(n)} - 1 \equiv 0$ has exactly $\varphi(n)$ roots. The primitive roots are then the roots that are **not** roots of $x^d - 1 \equiv 0$ where $d|\varphi(n)$.

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

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

Now 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_1q_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, thus the number of primitive roots are

$$q_1q_2 - q_1 - q_2 + 1 = (q_1 - 1)(q_2 - 1)$$
$$= \varphi(q_1q_2)$$
$$= \varphi(\varphi(n))$$

Now what happens if $\varphi(n)$ has three distinct prime factors? we do the same, we start with $q_1q_2q_3$ as the total number of roots, we then remove the ones already covered by q_1q_2, followed by q_1q_3 and finally q_2q_3. But in doing so we are again over counting because while removing the roots of $x^{q_1q_2} \equiv 1$ 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 $x^{q_1q_3} \equiv 1$ we again remove the roots of $x^{q_1} \equiv 1$, so we need to add them back in.

$$q_1q_2q_3 - q_1q_2 - q_1q_3 - q_2q_3 + q_1 + q_2 + q_3$$

But as we are removing roots and adding back over counted ones, 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

$$q_1q_2q_3 - q_1q_2 - q_1q_3 - q_2q_3 + q_1 + q_2 + q_3 - 1 = (q_1 - 1)(q_2 - 1)(q_3 - 1)$$
$$= \varphi(\varphi(n))$$

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

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

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

$$q_1^{a_1} q_2^{a_2} q_3^{a_3} - q_1^{a_1} q_2^{a_2} q_3^{a_3-1} - q_1^{a_1} q_2^{a_2-1} q_3^{a_3} - q_1^{a_1-1} q_2^{a_2} q_3^{a_3}$$
$$+ q_1^{a_1} q_2^{a_2-1} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3}$$

but just like before 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 again

$$q_1^{a_1} q_2^{a_2} q_3^{a_3} - q_1^{a_1} q_2^{a_2} q_3^{a_3-1} - q_1^{a_1} q_2^{a_2-1} q_3^{a_3} - q_1^{a_1-1} q_2^{a_2} q_3^{a_3}$$
$$+ q_1^{a_1} q_2^{a_2-1} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2} q_3^{a_3-1} + q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3}$$
$$- q_1^{a_1-1} q_2^{a_2-1} q_3^{a_3-1}$$

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 $x^3 - 1$ are already covered by the roots of $x^{3^2} - 1$ and so on.

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. We will then proceed through induction to prove it for any prime n.

Since $\varphi(\varphi(n))$ can never be zero and as long as $\mathbb{Z}/n\mathbb{Z}$ is a field, there's always exactly $\varphi(\varphi(n))$ primitive roots, since in this case n is prime $\mathbb{Z}/n\mathbb{Z}$ is guaranteed to be a field, so we have also not only proven that there are always primitive roots modulo a prime p but also how many there are.

Composite Conundrum

So we have proved that every off prime p has $\varphi(\varphi(p))$ primitive roots, what about composite numbers? First we tackle the case of $n = p^\alpha$.

Here $\varphi(n) = p^{\alpha-1}(p-1)$, so we tackle the problem of $x^d - 1 \equiv 0 \pmod{p^\alpha}$ with $d \mid \varphi(n)$ in three steps, first, when $d \mid p^{\alpha-1}$, second $d \mid (p-1)$ 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 therefore $d = 3$. If we cube all $a \in \mathbb{Z}/3^2\mathbb{Z} = \{1, 2, 3, \ldots, 3^2 = 9\}$ 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 seems like any number $a = 1 + x \cdot (3^2/3)$ will have $a^3 = \{1 + x \cdot (3^2/3)\}^3 \equiv 1 \pmod{3^2}$, so the generic formula when $d = p^\beta$, $\beta \leq \alpha - 1$ is $a = 1 + x \cdot p^{\alpha-\beta}$. Exponentiating to the dth 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 exponentiation above, we will bifurcate our discussion into binomial coefficients.

Proposition E.0. First, for $j > 0$

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

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

Proof. Let's rewrite the binomial as

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

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, let's see this with a concrete example, take $p^n = 5^2$ and $j = 7$, we then get

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

The reason behind this is 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 coeffcient 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 $(p, (p^{n-r} - 1)) = 1$. 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.0.1. For 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

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

6

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

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

therefore

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

Going back to our proposed solution $(1 + x \cdot p^{\alpha-\beta})^{p^\beta}$, utilizing Proposition E.0.1 with $m = \alpha - \beta$ and $n = \beta$ we get

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

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 $0 \le x < p^\beta$, meaning we have p^β 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 Littler 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.0.1, 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

$$1 + x'p^{\alpha-1} + vp^\alpha = 1 + wp^\alpha$$
$$x' = p(w - v)$$
$$p \mid x'$$

7

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

$$1 + x'' p^{\alpha - 2} + v' p^{\alpha - 1} = 1 + w' p^\alpha$$
$$x'' = p(pw' - v')$$
$$p \mid x''$$

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 still $1 + x \cdot p^{\alpha - \beta}$, 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 $1 + x \cdot p^{\alpha - \beta - 1}$. So we have shown that $x^{p^\beta} - 1 \equiv 0$ has exactly p^β solutions.

Next case is when $d | (p - 1)$, this one is a bit trickier and we need 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 case by case.

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, then a has to satisfy

$$a^d \equiv 1 \pmod{p^2}$$
$$\rightarrow a^d \equiv 1 \pmod{p}$$

so a is also a root $\pmod{p}$ this means that it is of the form $a + np$, our task is to see whether we can find such n, (a is guaranteed by Proposition 2.5.5). Let's see how this works

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

8

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

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

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.

So we have the following solutions

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

however, for $s \geq 1$, $a + np + sp^2$ is bigger than p^2, so we only have one such $a < p^2$ (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 is complete.

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

The proofs above give us an idea on how to prove that 2^α with $\alpha \geq 3$ doesn't have primitive roots. Say we elevate the roots of $x^2 - 1 \pmod{4}$ to modulo 8 just like before, we will get 4 roots, 1, 3, 5, 7, but $x^4 - 1 \pmod{8}$ only has 4 roots, but they are already covered by $x^2 - 1$, so 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 $x^4 - 1 \pmod{16}$ and they are also all the roots of $x^8 - 1 \pmod{16}$ so 16 has no primitive roots and so on. Let's see this in detail.

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

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 $8 \to 16$,

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

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

$$(a + 8)^2 = a^2 + 16a + 64 \qquad a^2 = 1 + 8m$$
$$\to \equiv 1 + 8m \pmod{16}$$

and so $(a + 8)^2 \equiv 1 \pmod{16}$ as well. And now we can 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 :)

So we are basically saying that all odd numbers $< 2^\alpha$ are roots of $x^{2^{\beta-1}} - 1 \pmod{2^\alpha}$ but again we also know that the roots of $x^{2^\beta} - 1 \pmod{2^\alpha}$ must also be a root of $x^{2^\beta} - 1 \pmod 2$, which is all the odd numbers less than 2^α, so we have covered all possible roots of $x^{\varphi(2^\alpha)} - 1 \pmod{2^\alpha}$. And we see why it doesn't work for $\alpha = 2$, this is because $\varphi(2)/2 = 1$ and $x^1 - 1$ can only have one root and not two.

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

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 above two :) Let's denote $d = xy$ with $x | p^{\alpha-1} \to x = p^\beta$ 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 first we 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

$$(a + w \cdot p^{\alpha-\beta})^{xy} = (a + w \cdot p^{\alpha-\beta})^{p^\beta y}$$

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

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

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

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

$$b^{xy} = (b^y)^{p^\beta} \equiv 1 \pmod{p^\alpha}$$

$$\rightarrow (b^y)^{p^\beta} \equiv 1 \pmod{p^\delta} \qquad 0 \le \delta < \alpha$$

but by Fermat's Little Theorem the only solution for the above is $b^y \equiv 1 \pmod{p}$ but this is what we have by extending these roots for every mod $p^{\alpha-\beta}$ so there are no other roots.

For $2p^\alpha$ we can repeat the whole process again or we can just utilize the following fact that if the order of x modulo a is o_a and the order of x mod b is o_b and $\gcd(a,b) = 1$ then the order of x mod ab is $\mathrm{lcm}(o_a, o_b)$.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

$$(a + n \cdot 2)^2 = a^2 + 4an + 4n^2$$

$$= 1 + 2m + 4an + 4n^2$$

$$\rightarrow 1 + 2m + 4an \equiv 1 \pmod 4$$

$$m + 4an = 2k$$

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

11