Primitive Roots modulo $p^n$

Prof. Weibel
Math 356:01 (Fall 2009)
Thursday, November 16, 2009

If $p \sim 10^{100}$ then the fraction of primitive roots mod $p$ is $\phi(p-1)/(p-1)$, which is at least $1/2$. So randomly picking 10 numbers under $p$, one is almost certain to be a primitive root modulo $p$. Unless you are Schrödinger ...

If $r$ is a primitive root mod $p$, there are $p$ numbers in $\mathbb{Z}/p^2$ which are $\equiv r \pmod{p}$. If we pick one at random, the odds that it is not a primitive root modulo $p^2$ are only 1 in $p$. So if $p \sim 10^{100}$ you can be pretty sure any lift you pick will work.

**Theorem.** Let $p$ be an odd prime and $r$ a primitive root mod $p$. Then all but one of the numbers $r + ap$ ($a = 0, 1, ..., p-1$) are primitive roots mod $p^2$.

**Example.** 2 is a primitive root modulo 5, so 4/5 of the numbers $r$ are primitive roots modulo 25. In fact, 7 isn’t a primitive root: $7^2 \equiv -1$ and $7^4 = 2401 \equiv 1 \pmod{25}$.

**Proof.** Write $x = r + ap$. Since $x^i \equiv r^i \pmod{p}$, the order of $x$ mod $p^2$ is divisible by the order of $r$ modulo $p$, i.e., $p-1$. Since every $y$ satisfies $y^{p(p-1)} \equiv 1 \pmod{p^2}$, $x$ is a primitive root if and only if $x^{p-1} \not\equiv 1 \pmod{p^2}$. Now $r^{p-1} \equiv 1 \pmod{p}$, say $r^{p-1} = 1 + bp \pmod{p^2}$ for some $b$ (which is unique modulo $p$). We compute:

$$x^{p-1} = r^{p-1} + (p-1)x^{p-2}(ap) + \left(\frac{p-1}{2}\right)x^{p-3}b^2p^2 + \ldots + b^{p-1}p^{p-1}$$

and all but the first two terms are divisible by $p^2$. Thus $x^{p-1} \equiv 1 + [b - ax^{p-2}]p \pmod{p^2}$. So $x^{p-1} \equiv 1$ exactly when $a = bx^{(p-2)}$. There is just one choice of $a$ (and hence of $x = r + ap$) for which this holds. □

**Theorem.** Let $p$ be an odd prime. If $r$ is a primitive root modulo $p^2$ then $r$ is a primitive root modulo $p^n$ for all $n \geq 2$.

**Proof.** We show by induction on $n$ that $r$ is a primitive root modulo $p^n$, the base case $n = 2$ being the hypothesis. So assume that $r$ is a primitive root modulo $p^{n-1}$. Set $e = \phi(p^{n-1}) = p^{n-2}(p-1)$, and note that $e/p = \phi(p^{n-2})$, $pe = \phi(p^n)$.

Since $r^i \not\equiv 1 \pmod{p^{n-1}}$ unless $e$ divides $i$, the order of $r$ is divisible by $e$. Since $y^{pe} \equiv 1 \pmod{p^n}$ by Euler’s Theorem, the order of $r$ divides $pe$. Thus $r$ is a primitive root modulo $p^n$ if and only if $r^e \not\equiv 1 \pmod{p^n}$.

The inductive hypothesis that $r$ is a primitive root modulo $p^{n-1}$ is equivalent to $r^{e/p} \not\equiv 1 \pmod{p^{n-1}}$. On the other hand, since $e/p = \phi(p^{n-2})$ we know that $r^{e/p} \equiv 1 \pmod{p^{n-2}}$. Thus we can write $r^{e/p} = 1 + ap^{n-2}$ for some $a \not\equiv 0 \pmod{p}$.

We may now compute:

$$r^e = (r^{e/p})^p = (1 + ap^{n-2})^p = 1 + ap^{n-1} + \left(\frac{p}{2}\right)a^2p^{2(n-1)} + \ldots \equiv 1 + ap^{n-1}.$$

Thus $r^e \not\equiv 1$ modulo $p^n$, and $r$ is a primitive root mod $p^n$. But induction, $r$ is a primitive root modulo $p^n$ for all $n \geq 2$. □