Cyclicity of $(\mathbb{Z}/p^n)^*$ for an odd prime p.

THEOREM. (Gauss.) *Let p be an odd prime. Then for all $n > 0$, $(\mathbb{Z}/p^n)^*$, the group of units in $\mathbb{Z}/p^n$, is cyclic.*

Proof. We saw in class that $(\mathbb{Z}/p)^*$ is cyclic. Let x be a generator, i.e., an element of order $p-1$. We show first that either x or $x+p$ has order $|(\mathbb{Z}/p^2)^*| = p(p-1)$ in $(\mathbb{Z}/p^2)^*$—so that $(\mathbb{Z}/p^2)^*$ is cyclic.

If x has order a in $(\mathbb{Z}/p^2)^*$, then a divides $|(\mathbb{Z}/p^2)^*| = p(p-1)$. Moreover, $x^a \equiv 1 \pmod{p}$, and so $p-1$ divides a. Thus $a = p(p-1)$ or $a = (p-1)$. In the first case we are done. In the second case, the same reasoning shows that $(x+p)$ has order $p(p-1)$ or $(p-1)$. But since p^2 doesn't divide px^{p-2}, the binomial expansion gives

$$(x+p)^{p-1} \equiv x^{p-1} + (p-1)px^{p-2} \equiv 1 - px^{p-2} \not\equiv 1 \pmod{p^2},$$

and so $x+p$ must have order $p(p-1)$ (and similarly, so does $x+bp$ for $0 < b < p$).

Next we prove for $n \geq 2$ that *if z is a generator of $(\mathbb{Z}/p^n)^*$ then z is a generator of $(\mathbb{Z}/p^{n+1})^*$*. Since we have seen that there is a generator z ($= x$ or $x+p$) when $n = 2$, it will follow by induction that z is a generator of $(\mathbb{Z}/p^n)^*$ for all $n \geq 2$, whence the desired conclusion.

LEMMA. *For any y and $n \geq 1$,*

$$y^p \equiv 1 \pmod{p^{n+1}} \iff y \equiv 1 \pmod{p^n}.$$

Proof. If either $y^p \equiv 1 \pmod{p^{n+1}}$ or $y \equiv 1 \pmod{p^n}$ then since $y \equiv y^p \pmod{p}$, therefore $y \equiv 1 \pmod{p}$, whence p divides $y^{p-1} + y^{p-2} + \cdots + y + 1 = (y^p - 1)/(y-1)$. So if $y-1$ is divisible by p^n then $y^p - 1$ is divisible by p^{n+1}.

The converse is proved by induction. The case $n = 1$ has been shown in the preceding paragraph. So suppose $n \geq 1$, and that if $y^p - 1$ is divisible by p^{n+1} then $y-1$ is divisible by p^n (inductive hypothesis). To go from n to $n+1$, suppose $y^p - 1$ is divisible by p^{n+2}, hence by p^{n+1}. Then by assumption, $y-1$ is divisible by p^n, that is, $y = 1 + kp^n$ for some k; and the binomial expansion gives

$$y^p = 1 + pkp^n + (p(p-1)/2)k^2p^{2n} + \cdots \equiv 1 + kp^{n+1} \pmod{p^{n+2}},$$

Since $y^p - 1$ is divisible by p^{n+2} therefore k is divisible by p, and so $y - 1 = kp^n$ is divisible by p^{n+1}. □

Returning to the main proof, suppose that z has order $|(Z/p^n)^*| = p^{n-1}(p-1)$ in $(\mathbb{Z}/p^n)^*$. Arguing as above in the case $n = 2$, we see that the order of z in $(\mathbb{Z}/p^{n+1})^*$ is either $p^n(p-1)$—in which case z is indeed a generator of $(\mathbb{Z}/p^{n+1})^*$—or $p^{n-1}(p-1)$. In the second case, the Lemma, with $y = z^{p^{n-2}(p-1)}$, would give that $z^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n}$, contradicting the assumption on the order of z. Thus the second case cannot occur, and the theorem is proved. □

Remarks. (a) The Lemma fails for $p = 2$. For example, $7^2 \equiv 1 \pmod{16}$, but $7 \not\equiv 1 \pmod{8}$.

Where does the proof break down in this case?

(b) The numbers 19 and 31 generate $(\mathbb{Z}/7)^*$, but don't generate $(\mathbb{Z}/49)^*$.

However, in less than 20 minutes on hardy, Mathematica calculates that if p is one of the first ten million primes, then the *smallest* positive generator of $(\mathbb{Z}/p)^*$ does generate $(\mathbb{Z}/p^2)^*$, with the *single exception* $p = 40487$, for which 5 generates the units mod p but not mod p^2.

Can you explain this? (I can't.)