# CLASS 21, GIVEN ON 11/08/2010, FOR MATH 25

## 1. Finding primitive roots in $U_{p^2}$

In the previous class, we saw that $U_p$ is cyclic, and so has primitive roots. We now want to show how we can use this fact to show that $U_{p^2}$ is cyclic.

Suppose $g$ is a primitive root mod $p$. If $g$ is also a primitive root mod $p^2$, then $U_{p^2}$ is cyclic and we are done. So suppose that $g$ is a primitive root mod $p$ but not $p^2$. We will show that $g+p$ is then primitive mod $p^2$.

Because $g$ is primitive mod $p$, this tells us that the order of $g$ mod $p$ is $p-1$. In particular, this tells us that the order of $g$ mod $p^2$ is at least $p-1$. Indeed, because none of $g, g^2, \ldots, g^{p-2}$ is congruent to $1 \mod p$, there is no way they can be congruent to $1 \mod p^2$ either. Suppose that $d$ is the order of $g$ mod $p^2$. Since $U_{p^2}$ has size $\phi(p^2) = p(p-1)$, this means $d \mid p(p-1)$. We claim $p \nmid d$. For suppose $p \mid d$. We also know that $g^d \equiv 1 \mod p^2$, which implies $g^d \equiv 1 \mod p$, or that $(p-1) \mid d$. Since $p, p-1$ are coprime, this would imply that $p(p-1) \mid d$, which in combination with what we already know implies $d = p(p-1)$. But if this is the case, $g$ is a primitive root mod $p^2$, contradicting our original assumption.

So this implies that $p \nmid d$. Since $p, p-1$ are coprime, and $d \mid p(p-1)$, this implies that $d \mid (p-1)$. However, notice that we already know that $d \geq p-1$. This implies that $d = p-1$. So if $g$ is a primitive root mod $p$ but is not a primitive root mod $p^2$, then $g$ has order $p-1$ mod $p^2$; in other words, $g^{p-1} \equiv 1 \mod p^2$.

The claim is that $g+p$ is a primitive root mod $p^2$. Indeed, first notice that $g+p$ is still a primitive root mod $p$, since $g+p \equiv g \mod p$. So the above analysis applied to $g+p$ in place of $g$ shows that the order of $g+p$ is either equal to $p(p-1)$ or $p-1$, depending on whether $g+p$ is primitive mod $p^2$ or not. So we calculate $(g+p)^{p-1} \mod p^2$, using the binomial theorem:

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \ldots + p^{p-1} \equiv g^{p-1} + p(p-1)g^{p-2} \mod p^2.$$

We know that $g^{p-1} \equiv 1 \mod p^2$. On the other hand, notice that $p(p-1)g^{p-2} \not\equiv 0 \mod p^2$: indeed, even though $p \mid p(p-1)g^{p-2}$, $p^2 \nmid p(p-1)g^{p-2}$, because $p$ is prime, and is coprime to both $p-1$ and $g$. Therefore, $(g+p)^{p-1} \not\equiv 1 \mod p^2$, which shows that $g+p$ is a primitive root mod $p^2$.

## 2. Finding primitive roots in $U_{p^e}$, $p$ odd

We now know that both $U_p, U_{p^2}$ are cyclic. In the former case, we don't really have an efficient method of finding primitive roots, but for $U_{p^2}$, we can find primitive roots quickly assuming we know a primitive root for $U_p$. (Namely, if $g$ is primitive mod $p$, then either $g$ or $g+p$ is primitive mod $p^2$.) When $p$ is odd, we can extend this to $U_{p^e}$ for $e \geq 1$.

To prove this, we will proceed by induction. Suppose that we know that $U_{p^e}$ is cyclic, for odd $p$, $e \geq 2$. We will show that $U_{p^{e+1}}$ is also cyclic.

Let $g$ be a primitive root mod $p^e$. The claim is that $g$ is still a primitive root mod $p^{e+1}$. First, notice that $g^{\phi(p^e)} \equiv 1 \mod p^e$, and because $g$ is primitive, $g^k \not\equiv 1 \mod p^e$ if $1 \leq k < \phi(p^e)$. Since $\phi(p^e) = p^{e-1}(p-1)$, this implies that $g^{p^{e-2}(p-1)} \not\equiv 1 \mod p^e$. However, $g^{p^{e-2}(p-1)} = g^{\phi(p^{e-1})} \equiv 1 \mod p^{e-1}$, so $g^{p^{e-2}(p-1)} = 1 + kp^{e-1}$, for some integer $k$ with $p \nmid k$.

The goal is to show that $g^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}$. This will show that $g$ is primitive mod $p^{e+1}$. Indeed, if $d$ is the order of $g$ mod $p^{e+1}$, then we have $\phi(p^e) \mid d$. On the other hand, $d \mid \phi(p^{e+1})$. This means that $p^{e-1}(p-1) \mid d, d \mid p^e(p-1)$, and therefore $d = p^{e-1}(p-1)$ or $p^e(p-1)$. If the latter is true, then $g$ is primitive mod $p^{e+1}$, and the latter is true if $d \neq p^{e-1}(p-1)$, which is equivalent to showing that $g^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}$.

The idea is similar to that in the first section. We apply the binomial theorem to $g^{p^{e-1}(p-1)}$, in the form $(g^{p^{e-2}(p-1)})^p$, with $g^{p^{e-2}(p-1)} = 1 + kp^{e-1}$. The binomial theorem gives

$$(1 + kp^{e-1})^p = 1 + pkp^{e-1} + \binom{p}{2} k^2 p^{2(e-1)} + \ldots + k^p p^{p(e-1)}.$$

Consider this expression mod $p^{e+1}$. We claim that every term past the second is divisible by $p^{e+1}$. Indeed, past the third term, the power of $p$ is $i(e-1), i \geq 3$, and $i(e-1) \geq e+1$ is clear. The third term is divisible by exactly $p^{2(e-1)+1}$, since $\binom{p}{2}$ is divisible by $p$ if $p$ is odd. On the other hand, we see that $2(e-1)+1 = 2e-1 \geq e+1$, since $e \geq 2$. So all terms except the first two are divisible by $p^{e+1}$. This proves that

$$(1 + kp^{e-1})^p \equiv 1 + kp^e \mod p^{e+1}.$$

However, notice that we know $p \nmid k$. Therefore $1 + kp^e \nmid 1 \mod p^{e+1}$, as desired.