Week 10 Summary

Lecture 19

The following proposition is proved by exactly the same argument used to prove the second statement in the Fermat-Euler Theorem (see Lecture 12, Week 6).

***Proposition:** Let a, $n \in \mathbb{Z}^+$, and suppose that $\gcd(a, n) = 1$. Let $m = \operatorname{ord}_n(a)$. Then $a^k \equiv 1 \pmod{n}$ if and only if $m|k$.

We made use of this in Lecture 18 in the proof of the following result.

***Proposition:** Let p be prime and q any prime divisor of $p-1$. Let $p-1 = q^n K$ where K is not divisible by q. Then there is some integer t whose order modulo p is q^n.

The point is that since $(t^K)^{q^n} = t^{p-1} \equiv 1 \pmod{p}$ the preceding proposition tells us that $\operatorname{ord}_p(t^K)$ is a divisor of q^n for all nonzero t in $\mathbb{Z}_p$. But the only divisor of q^n that is not also a divisor of q^{n-1} is q^n itself; so if there is no t such that $\operatorname{ord}_p(t^K) = q^n$ then $(t^K)^{q^{n-1}} - 1 = 0$ for all nonzero $t \in \mathbb{Z}_p$. This is impossible since a polynomial equation of degree less than $p-1$ cannot have $p-1$ roots in $\mathbb{Z}_p$.

***Theorem:** Let p be a prime. There there is an integer t such that $\operatorname{ord}_p(t) = p-1$. That is, there exists a primitive root modulo p.

If we factorize $p-1$ as $q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$, where the q_i are distinct primes, then the preceding proposition tells us that for each i there exists an element t_i such that $\operatorname{ord}_p(t_i) = q_i^{n_i}$. Now in Question 4 of Tutorial 6 it was shown that if $\operatorname{ord}_n(x) = a$ and $\operatorname{ord}_n(y) = b$ and $\gcd(a, b) = 1$, then $\operatorname{ord}_n(xy) = ab$. By repeated application of this we deduce that

$$\operatorname{ord}_p(t_1 t_2 \cdots t_r) = \operatorname{ord}_p(t_1) \operatorname{ord}_p(t_2) \cdots \operatorname{ord}_p(t_r) = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r} = p - 1,$$

so that $t = t_1 t_2 \cdots t_r$ is a primitive root.

It turns out that a primitive root modulo n exists whenever n is a power of an odd prime, or twice a power of an odd prime, or when $n = 2$ or 4, but not in any other cases. We shall not prove this, although Q. 2 of Tutorial 9 and Q. 2 of Tutorial 10 should enable the student to see why no primitive root can exist for numbers n that are divisible by two distinct odd primes.
Remember that a primitive root modulo n (by definition) is a an integer t such that $\operatorname{ord}_n(t) = \varphi(n)$. And $\varphi(n) = n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right) \cdots \left(\frac{p_r-1}{p_r}\right)$. So, for example, a primitive root modulo 50 is an integer t with $\operatorname{ord}_{50}(t) = \varphi(50) = 50 \times \frac{1}{2} \times \frac{4}{5} = 20$. The powers of t then give all 20 elements of $\mathbb{Z}_{50}$ that are coprime to 50.
It turns out to be quite easy, given a primitive root modulo an odd prime p, to construct primitive roots modulo higher powers of p. We shall not go into the details of this, but content ourselves with one example. It is easily checked that

2 is a primitive root modulo 11. Suppose we now wish to find a primitive root modulo 11^2. It seems reasonable that a primitive root modulo 11^2 will also be a primitive root modulo 11; so we look amongst the integers mod 11^2 that are congruent to 2 (mod 11). This gives us 11 possible candidates: 2, 13, 24, 35, 46, 57, 68, 79, 90, 101 and 112. If t is any one of these, and if $m = \mathrm{ord}_{121}(t)$ then $t^m \equiv 1 \pmod{11^2}$, which certainly implies that $t^m \equiv 1 \pmod{11}$. But $t \equiv 2 \pmod{11}$; so $2^m \equiv 1 \pmod{11}$, and so $\mathrm{ord}_{11}(2)$ is a divisor of m. So $10|m$. But the Fermat-Euler Theorem also tells us that $\mathrm{ord}_{121}(t)$ is a divisor of $\varphi(121) = 110$, and since the only multiples of 10 that are divisors of 110 are 10 and 110, it follows for each of our 11 candidates t that $\mathrm{ord}_{121}(t)$ is either 10 or 110. It turns out—and this is a particular instance of a general fact—that all but one of them have order 110. Only one of the candidates fails to be a primitive root modulo 121. In particular, it is easily verified that 2 is a primitive root: $2^{10} = 1024 \equiv 56 \not\equiv 1 \pmod{121}$; so $\mathrm{ord}_{121}(2) \neq 10$, and therefore $\mathrm{ord}_{121}(2) = 110$, as required.

Our next topic is the inverstigation of quadratic residues modulo p, where p is an odd prime number. *Quadratic residue* is the traditional term in number theory for elements of $\mathbb{Z}_p^*$ that have square roots in $\mathbb{Z}_p^*$. Thus the set of quadratic residues modulo p is the set

$$\mathcal{S}_p = \{\, x^2 \mid x \in \mathbb{Z}_p^* \,\} = \{\, t \in \mathbb{Z}_p^* \mid t = a^2 \text{ for some } a \in \mathbb{Z}_p^* \,\}.$$

The elements of the set

$$\mathcal{N}_p = \{\, t \in \mathbb{Z}_p^* \mid x^2 = t \text{ has no solution } x \in \mathbb{Z}_p^* \,\}$$

are called *quadratic non-residues* modulo p.

For example, modulo 7 the quadratic residues are 1, 2 and 4, while the quadratic residues are 3, 5 and 6. Since every nonzero element that has a square root has exactly two square roots, the number of elements with square roots must be half the total number of elements, or $(p-1)/2$. If we write the elements of $\mathbb{Z}_p$ as $-(p-1)/2, -(p-3)/2, \ldots, -2, -1, 0, 1, 2, \ldots, (p-3)/2, (p-1)/2$ then we see that the distinct quadratic residues are precisely $1^2, 2^2, \ldots, ((p-1)/2)^2$, since $(-i)^2$ is equal to i^2.