Math 328K. Fall 2025
Some solutions to Homework # 9

Prof. Hector E. Lomeli

Section 9.1. Exercise 8. We have that $\phi(20) = 8$ and

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

We can compute the order of all these elements. We find that $\text{ord}_{20}(1) = 1$,

$$\text{ord}_{20}(9) = \text{ord}_{20}(11) = \text{ord}_{20}(19) = 2,$$

and

$$\text{ord}_{20}(3) = \text{ord}_{20}(7) = \text{ord}_{20}(13) = \text{ord}_{20}(17) = 4.$$

None of these has order 8, so there are no primitive roots.

Section 9.1. Exercise 12. Let $r = \text{ord}_n(a)$, $s = \text{ord}_n(b)$, and $t = \text{ord}_n(ab)$. We know that $(r, s) = 1$. First, we notice that

$$(ab)^{rs} = (a^r)^s(b^s)^r \equiv 1 \pmod{n}.$$

This implies that $\text{ord}_n(ab)|rs$, or $t|rs$. We also have that

$$(a^t)(b^t) = (ab)^t \equiv 1 \pmod{n}.$$

This implies that

$$(a^{st})(b^s)^t \equiv 1 \pmod{n}.$$

Given that $s = \text{ord}_n(b)$, we conclude that $a^{st} \equiv 1 \pmod{n}$ and hence $r|st$. However, the numbers s and r are coprime so $r|t$. In the same way, we conclude that $s|t$. As a consequence, $[r, s]$ divides t and since $(r, s) = 1$, we get $rs|t$.

Given that $rs|t$ and $t|rs$, we conclude that $t = rs$.

Section 9.1. Exercise 20. a) Let $t = \text{ord}_p(2)$. First, we will prove that $t \mid 2^{n+1}$. We have that

$$2^{2^n} \equiv -1 \pmod{F_n}.$$

This implies that

$$2^{2^{n+1}} \equiv (-1)^2 = 1 \pmod{F_n}.$$

and therefore

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

From this we conclude that $t \mid 2^{n+1}$.

To get that $t = 2^{n+1}$, we will use a proof by way of contradiction. The number t has to be of the form $t = 2^k$ for some $0 \leq k \leq n + 1$. Suppose BWOC that $k \leq n$. Then $t \mid 2^n$.

We will prove that this leads to a contradiction. If $t \mid 2^n$, then 2^n is of the form $2^n = \ell \cdot t$. Given that $t = \text{ord}_p(2)$, we find that

$$2^t \equiv 1 \pmod{p},$$

and hence

$$2^{2^n} = 2^{\ell \cdot t} = \left(2^t\right)^\ell \equiv 1 \pmod{p}.$$

We conclude that $p \mid 2^{2^n} - 1$. However, we also have the assumption that $p \mid F_n = 2^{2^n} + 1$ and this would imply that $p \mid 2$. This is a contradiction, because all the primes that divide F_n are odd.

The original assumption is incorrect, so we have that $t = 2^{n+1}$.

Section 9.1. Exercise 20. b) We have that F_n is odd, so all its prime divisors are odd. In particular, we have that $(2,\, p) = 1$. Using FLT, we get that

$$2^{p-1} \equiv 1 \pmod{p}.$$

This implies that $\text{ord}_p(2) \mid p - 1$. Using part **a)**, we conclude that $2^{n+1} \mid p - 1$. From this, we conclude that p must be of the form

$$p = 2^{n+1} \cdot \ell + 1,$$

for some $\ell \in \mathbb{N}$.

Section 9.2. Exercise 8. Let $\ell = (p-1)/2 = 2k$ and $z = r^\ell$. We have that

$$z^2 \equiv r^{2\ell} \equiv r^{p-1} \equiv 1 \pmod{p}.$$

Given that $\text{ord}_p(r) = p - 1$, and $\ell < p - 1$, we have that $z \not\equiv 1$. This implies that

$$z \equiv -1 \pmod{p},$$

and therefore

$$-r \equiv z \cdot r = r^{\ell+1} = r^{2k+1} \pmod{p}.$$

We notice that $(2k+1,\, \text{ord}_p(r)) = (2k+1,\, p-1) = (2k+1, 4k) = 1$. This implies that

$$\text{ord}_p(-r) = \text{ord}_p(r^{2k+1}) = \frac{\text{ord}_p(r)}{(2k+1,\, \text{ord}_p(r))} = \text{ord}_p(r) = p - 1.$$

We conclude that $-r$ is also a primitive root of p.

Section 9.2. Exercise 9. The prime p is of the form $p = 4k + 1$. Let r be a primitive root of p. We know that $r^{p-1} \equiv 1 \pmod{p}$. If we define $x = r^k$, then

$$x^4 = r^{4k} \equiv 1 \pmod{p}.$$

This implies that $p \mid (x^2+1)(x^2-1)$. By definition of primitive root,

$$x^2 = r^{2k} \not\equiv 1 \pmod{p}$$

and hence $p \nmid x^2 - 1$. Using Euclid's lemma, $p \mid x^2 + 1$ and therefore

$$x^2 = r^{2k} \equiv -1 \pmod{p}.$$