Homework 13

Chris Powell

A. Silverman 28.3.

(a) Compute $e_m(2)$ for each odd number $11 \leqslant m \leqslant 19$.

As $m = 11$ is prime, the Order Divisibility Property implies

$$e_{11}(2) \mid \varphi(11) = 11 - 1 = 10.$$

But $\{ x \in \mathbb{N} : x \mid 10 \} = \{ 1, 2, 5, 10 \}$. Observe that

$$\begin{aligned} \left[2^1\right]_{11} &= [2]_{11} \neq [1]_{11} \\ \left[2^2\right]_{11} &= [4]_{11} \neq [1]_{11} \\ \left[2^5\right]_{11} &= [10]_{11} \neq [1]_{11} \\ \left[2^{10}\right]_{11} &= [1]_{11}. \end{aligned}$$

Hence $e_{11}(2) = 10$, so 2 is a primitve root modulo 11.

As $m = 13$ is prime, the Order Divisibility Property implies

$$e_{13}(2) \mid \varphi(13) = 13 - 1 = 12.$$

But $\{ x \in \mathbb{N} : x \mid 12 \} = \{ 1, 2, 3, 4, 6, 12 \}$. Observe that

$$\begin{aligned} \left[2^1\right]_{13} &= [2]_{13} \neq [1]_{13} \\ \left[2^2\right]_{13} &= [4]_{13} \neq [1]_{13} \\ \left[2^3\right]_{13} &= [8]_{13} \neq [1]_{13} \\ \left[2^4\right]_{13} &= [3]_{13} \neq [1]_{13} \\ \left[2^6\right]_{13} &= [12]_{13} \neq [1]_{13} \\ \left[2^{12}\right]_{13} &= [1]_{13}. \end{aligned}$$

Hence $e_{13}(2) = \varphi(13)$, so 2 is a primitive root modulo 13.

Now $m = 15$ is not prime as $15 = 3 \cdot 5$. But

$$e_{15}(2) = \frac{e_3(2)e_5(2)}{\gcd\left(e_3(2), e_5(2)\right)}$$

since $\gcd(3,5) = 1$. Observe that

$$\begin{aligned} \left[2^1\right]_3 &= [2]_3 \neq [1]_3 & \left[2^1\right]_5 &= [2]_5 \neq [1]_5 \\ \left[2^2\right]_3 &= [4]_3 \neq [1]_3 & \left[2^2\right]_5 &= [4]_5 \neq [1]_5 \\ \left[2^3\right]_3 &= [2]_3 \neq [1]_3 & \left[2^3\right]_5 &= [3]_5 \neq [1]_5 \\ \left[2^4\right]_3 &= [1]_3 & \left[2^4\right]_5 &= [1]_5 \end{aligned}$$

So $e_3(2) = e_5(2) = 4$. Thus

$$e_{15}(2) = \frac{e_3(2)e_5(2)}{\gcd\left(e_3(2), e_5(2)\right)} = \frac{16}{4} = 4.$$

As $m = 17$ is prime, the Order Divisibility Property implies

$$e_{17}(2) \mid \varphi(17) = 17 - 1 = 16.$$

But $\{ x \in \mathbb{N} : x \mid 16 \} = \{1, 2, 4, 8, 16\}$. Observe that

$$\begin{aligned} \left[2^1\right]_{17} &= [2]_{17} \neq [1]_{17} \\ \left[2^2\right]_{17} &= [4]_{17} \neq [1]_{17} \\ \left[2^4\right]_{17} &= [16]_{17} \neq [1]_{17} \\ \left[2^8\right]_{17} &= [1]_{17}. \end{aligned}$$

Hence $e_{17}(2) = 8$, so 2 is not a primitve root modulo 17.

As $m = 19$ is prime, the Order Divisibility Property implies

$$e_{19}(2) \mid \varphi(19) = 19 - 1 = 18.$$

But $\{ x \in \mathbb{N} : x \mid 18 \} = \{ 1, 2, 3, 6, 9, 18 \}$. Observe that

$$\begin{aligned}
\left[2^1\right]_{19} &= [2]_{19} \neq [1]_{19} \\
\left[2^2\right]_{19} &= [4]_{19} \neq [1]_{19} \\
\left[2^3\right]_{19} &= [8]_{19} \neq [1]_{19} \\
\left[2^6\right]_{19} &= [16]_{19} \neq [1]_{19} \\
\left[2^9\right]_{19} &= [18]_{19} \neq [1]_{19} \\
\left[2^{18}\right]_{19} &= [1]_{19}.
\end{aligned}$$

Hence $e_{19}(2) = \varphi(19)$, so 2 is a primitve root modulo 19.

(b) Using the table (page. 221), find a formula for $e_{mn}(2)$ in terms of e_m and e_n whenever $\gcd(m,n)=1$.

Conjecture. If $\gcd(e_m(2), e_n(2))$, then

$$e_{mn}(2) = \frac{e_m(2)e_n(2)}{\gcd(e_m(2), e_n(2))}.$$

(c) Use your conjectural formula form (b) to find the value of e_{11227}. (Note that $11227 = 103 \cdot 109$).

Since $11227 = 103 \cdot 109$ and $\gcd(103, 109) = 1$, we satisfy the hypothesis of the conjecture. Note that $e_{103}(2) = 51$ and $e_{109}(2) = 36$. So the conjectured formula gives

$$e_{11227}(2) = \frac{e_{103}(2)e_{109}(2)}{\gcd(e_{103}(2), e_{109}(2))} = \frac{1836}{3} = 612.$$

(d) Prove that your conjectural formula in (b) is true.

Proof. Let $m, n \in \mathbb{Z}$ be relatively prime, and let

$$g = \gcd(e_m(2), e_n(2)).$$

By definition, $e_m(2)$ and $e_n(2)$ are the least positive integers satisfying $\left[2^{e_m(2)}\right]_m = [1]_m$ and $\left[2^{e_n(2)}\right]_n = [1]_n$, respectively. Observe that

$$\left[2^{\frac{e_m e_n(2)}{g}}\right]_m = \left[2^{e_m(2)}\right]_m^{\frac{e_n(2)}{g}} = [1]_m^{\frac{e_n(2)}{g}} = [1]_m.$$

Similarly, $\left[2^{\frac{e_m e_n(2)}{g}}\right]_n = [1]_n$. So $m, n \mid \left(2^{\frac{e_m e_n(2)}{g}} - 1\right)$. Moreover, as $\gcd(m,n) = 1$, we know

$$mn \mid \left(2^{\frac{e_m e_n(2)}{g}} - 1\right).$$

Thus $\left[2^{\frac{e_m e_n(2)}{g}}\right]_{mn} = [1]_{mn}$. But the Chinese Remainder Theorem implies that $[1]_{mn}$ can be written uniquely as $([1]_m, [1]_n)$. The result follows. ■

B. Silverman 28.4.

(a) Find all primitive roots modulo 13.

Suppose g is a primitive root modulo 13. Observe that

$$e_{13}(g^k) = \frac{e_{13}(g)}{\gcd(k, e_{13}(g))}$$

holds exactly when $\gcd(k, e_{13}(g)) = 1$. But

$$e_{13}(g) = \varphi(13) = 13 - 1 = 12,$$

and

$$\{\, k \in \mathbb{Z} \mid 2 \leqslant k \leqslant 12,\ \gcd(k, 12) = 1 \,\} = \{5, 7, 11\}.$$

Thus g^5, g^7, g^{11} are primitive roots modulo 13.

(b) For each number d dividing 12, list the a's with $1 \leqslant a < 13$ and $e_{13}(a) = d$.

Let $1 \leqslant d < 13$ be a divisor of 12. Then

$$d \in \{1, 2, 3, 4, 6, 12\}.$$

Let a be such that $e_{13}(a) = d$. This gives the following table:

d	a
1	1
2	12
3	3
4	6
6	12
12	2

C. Silverman 28.5.

(a) If g is a primitve root modulo 37, which of the numbers $g^2, g^3, \ldots, g^8$ are primitve roots modulo 37?

Suppose g is a primitive root modulo 37. Observe that

$$e_{37}(g^k) = \frac{36}{\gcd(k, 36)}$$

provided $\gcd(k, 36) = 1$. But

$$\{k \in \mathbb{Z} \mid 2 \leqslant k \leqslant 8,\ \gcd(k, 36) = 1\} = \{5, 7\}.$$

Thus g^5 and g^7 are primitive roots modulo 37.

(b) If g is a primitive root modulo p, develop an easy-to-use rule for determining if g^k is a primitive root modulo p, and prove the your rule is correct.

Proposition. If $\gcd(k, p-1) = 1$, then

$$e_p(g^k) = \frac{p-1}{\gcd(k, p-1)}.$$

Proof. Suppose g is a primitive root modulo p. Observe that

$$e_p(g^k) = \frac{e_p(g)}{\gcd(k, e_p(g))}.$$

But $e_p(g) = \varphi(p) = p - 1$. Thus,

$$e_p(g^k) = \frac{p-1}{\gcd(k, p-1)}.$$

■

(c) Suppose that g is a primitive root modulo the prime $p = 21169$. Use your rule from (b) to determine which of the numbers $g^2, g^3, \ldots, g^{20}$ are primitive roots modulo 21169.

D. Silverman 28.8. Let p be an odd prime and let g be primitive root modulo p.

(a) Prove that g^k is a quadratic residue modulo p if, and only if, k is even.

Proof. Suppose otherwise there is ℓ such that $\left[g^{2k+1}\right]_p = \left[a^2\right]_p$.

$$\left[\left(g^{\frac{p-1}{2}}\right)^2\right]_p = \left[g^{p-1}\right]_p = [1]_p .$$

Conversely, if $k = 2m$ for some $m \in \mathbb{Z}$, then

$$\left[g^k\right]_p = \left[g^{2\ell}\right]_p = \left[\left(g^{\ell}\right)^2\right]_p .$$

■

(b) Use (a) to give a quick proof that the product of two nonresidues is a residue, and more generally that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(c) Use (a) to give a quick proof of Euler's Criterion $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

E. Silverman 28.9. Suppose that q is a prime number that is congruent to 1 modulo 4, and suppose that the number $p = 2q + 1$ is also a prime number. Show that 2 is a primitive root modulo p. [*Hint*. Euler's Criterion and Quadratic Reciprocity will be helpful.]

F. Silverman 28.11. Write a computer program to compute $e_p(a)$, which is the smallest positive exponent e such that $a^e \equiv 1 \pmod{p}$. [Be sure to use the fact that if $a^e \not\equiv 1 \pmod{p}$ for all $1 \leqslant e \leqslant \frac{p}{2}$, then $e_p(a)$ is automatically equal to $p-1$.]

G. Silverman 28.14.

(a) For each number $2 \leqslant m \leqslant 25$, determine if there any primitive roots modulo m.

(b) Use your data from (a) to make a conjecture as to which m's have primtiive roots and which ones do not.

(c) Prove that your conjecture in (b) is correct.