18.781 Solutions to Problem Set 4, Part 2

1. (a) To find a primitive root mod 23, we use trial and error. Since $\phi(23) = 22$, for a to be a primitive root we just need to check that $a^2 \not\equiv 1 \pmod{23}$ and $a^{11} \not\equiv 1 \pmod{23}$.

$$2^{11} = 2^5 \cdot 2^5 \cdot 2 \equiv 9 \cdot 9 \cdot 2 \equiv -11 \cdot 2 \equiv 1 \pmod{23},$$

so 2 doesn't work.

$$3^{11} \equiv 3^3 \cdot 3^3 \cdot 3^3 \cdot 9 \equiv 4^3 \cdot 9 \equiv -5 \cdot 9 \equiv 1 \pmod{23},$$

so 3 doesn't work either.

$$5^{11} \equiv (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 \equiv -1 \pmod{23}$$

and $5^2 \equiv 2 \pmod{23}$, so 5 is a primitve root mod 23.

Now by the proof of existence of primitive roots mod p^2, using Hensel's lemma, only one lift of 5 will fail to be a primitive root mod 23^2. We need to check whether $5^{22} \equiv 1 \pmod{23^2}$:

$$\begin{aligned} 5^{22} &= (5^5)^4 \cdot 5^2 \equiv (3125)^4 \cdot 25 \\ &\equiv (-49)^4 \cdot 25 \equiv (2401)^2 \cdot 25 \\ &\equiv 288 \cdot 25 \equiv 323 \pmod{529}. \end{aligned}$$

So 5 is a primitive root mod 529.

(b) We have that

$$3^8 \equiv (3^4)^2 \equiv (-4)^2 \equiv -1 \pmod{17}.$$

Now the order of 3 mod 17 must divide $\phi(17) = 16$, and thus must be a power of 2. Clearly the order must be greater than 8, since otherwise the order would divide 8 and we would have $3^8 \equiv 1 \pmod{17}$. So the order of 3 mod 17 is exactly 16, which implies that 3 is a primitive root mod 17.

2. Since $2^m - 1$ and $2^n + 1$ are odd, any prime p dividing both must be an odd prime. We have $2^m \equiv 1 \pmod{p}$ and $2^n \equiv -1 \pmod{p}$, so the order of 2 mod p, say, h, divides m and is thus odd. But since $2^{2n} \equiv (2^n)^2 \equiv 1 \pmod{p}$, h must also divide n, so $2^n \equiv -1 \equiv 1 \pmod{p}$, contradiction. Therefore $\gcd(2^m - 1, 2^n + 1)$ can't have any prime divisors, so it must equal 1.

3. If k is not a power of 2, then some odd prime p divides k. Letting $k = mp$, we have

$$\begin{aligned} a^k + 1 &= a^{mp} + 1 \\ &= (a^m + 1)(a^{m(p-1)} - a^{m(p-2)} + \cdots - a^m + 1). \end{aligned}$$

It's easy to see that $1 < a^m + 1 < a^k + 1$, so $a^k + 1$ must be composite. Therefore for $a^k + 1$ to be prime, k must be a power of 2.

Now if $p | a^{2^n} + 1$ and $p \neq 2$ then p is odd, and $a^{2^n} \equiv -1 \pmod{p}$ implies that $a^{2^{n+1}} \equiv 1 \pmod{p}$. Note that $(a, p) = 1$. So the order of a mod p, say, h, divides 2^{n+1} and is thus a power of 2. But h cannot be less than or equal to 2^n, else we would have $2^{2n} \equiv -1 \equiv 1 \pmod{p}$, contradicting the assumption that p is odd. Therefore, $h = 2^{n+1}$. Then by Fermat's Little Theorem we have $2^{n+1} | p - 1$, i.e., $p \equiv 1 \pmod{2^{n+1}}$.

4. Since $a^{n-1} \equiv 1 \pmod{n}$, it follows immediately that $\gcd(a, n) = 1$. Let h be the order of a mod n. By definition h is the smallest positive integer such that $a^h \equiv 1 \pmod{n}$, so $h = n - 1$. Now Euler's theorem implies that $a^{\phi(n)} \equiv 1 \pmod{n}$. Thus, $h = n-1|\phi(n)$, which in particular means that $n - 1 \leq \phi(n)$. But since $n > 1$, we know that $\phi(n)$ is the number of elements in $\{1, \ldots, n-1\}$ which are coprime to n, so $\phi(n) \leq n - 1$. Hence $\phi(n) = n - 1$ and n is coprime to $1, 2, \ldots, n - 1$. Therefore, n must be prime.

5. We'll first show that if $a \equiv b \pmod{p(p-1)}$, then $a^a \equiv b^b \pmod{p}$. If a and b are both equivalent to 0 mod p then $a^a \equiv b^b \equiv 0 \pmod{p}$ is clear, since a and b are positive integers. So assume a, and thus b as well, is coprime to p. Writing $b = a + tp(p-1)$, we have

$$\begin{aligned} b^b &= (a + tp(p-1))^{a+tp(p-1)} \\ &\equiv a^{a+tp(p-1)} \\ &\equiv a^a \cdot (a^{p-1})^{tp} \\ &\equiv a^a \cdot (1)^{tp} \\ &\equiv a^a \pmod{p}. \end{aligned}$$

Now let the period of the sequence be h. From the above proof, h divides $p(p-1)$. We know that $a^a \equiv (a+th)^{a+th} \pmod{p}$ for all positive integers a, t. If we set $a = p$ and $t = 1$ we get $p^p \equiv (p+h)^{p+h} \pmod{p}$, which forces $h \equiv 0 \pmod{p}$. So letting $h = kp$, we have

$$a^a \equiv (a + tkp)^{a+tkp} \equiv a^{a+tkp} \pmod{p}$$

for every pair of positive integers a, t. If we take a to be a primitive root g mod p and again set $t = 1$, we get that $g^{kp} \equiv 1 \pmod{p}$, so $p - 1|kp$. Furthermore, $p - 1|k$ because $\gcd(p-1, p) = 1$. Therefore, $h = kp$ is divisible by $(p-1)p$. Since h also divides $p(p-1)$, it follows that $h = p(p-1)$.

6. We can assume that $0 < a < q$, otherwise divide out a/q and reset a as the remainder. Now if k is the order of 10 mod q then $q|10^k - 1$, so let $10^k - 1 = mq$ for some positive integer m. Then

$$\begin{aligned} \frac{a}{q} &= \frac{10^k a}{10^k q} \\ &= \frac{a(10^k - 1 + 1)}{10^k q} \\ &= \frac{a(10^k - 1)}{10^k q} + \frac{a}{10^k q} \\ &= \frac{am}{10^k} + \frac{a}{10^k q} \end{aligned}$$

Now note that $0 < am < qm \leq 10^m - 1$. So $\frac{am}{10^k}$ has a finite decimal expansion $0.m_1 m_2 \cdots m_k$ with k digits, and since the decimal expansion of $\frac{a}{10^k q}$ is just that of $\frac{a}{q}$ but shifted k digits to the right by adding k zeroes at the beginning, it's clear that $\frac{a}{q}$ will have the decimal expansion $0.m_1 \cdots m_k m_1 \cdots m_k m_1 \cdots m_k \cdots$. So the smallest period is a divisor of k. To show it's exactly k, suppose that $a/q = 0.r_1 \cdots r_l n_1 \cdots n_h n_1 \cdots n_h \cdots$, where h divides k. Multiplying by 10^l, we get

$$\frac{10^l a}{q} = r_1 \cdots r_l.n_1 \cdots n_h n_1 \cdots n_h \cdots$$

Subtracting off the integer part and replacing a by the remainder of $10^l a$ mod q (which doesn't change the fact that $(a, q) = 1$),

$$\frac{a}{q} = 0.n_1 \cdots n_h n_1 \cdots n_h \cdots$$

If n is the integer with decimal expansion $n_1 \cdots n_h$, this equation says $a/q = n/(10^h - 1)$. Then $(10^h - 1)a = nq$, so $a(10^h - 1) \equiv 0 \pmod{p}$. By definition of k, we must have $k|h$. Therefore $k = h$, finishing the proof.

18.781 Theory of Numbers
Spring 2012