1 Exercises

1.1

What are the orders of 3, 5, and 7, modulo 8?

All are of order 2.

1.2

What order can an integer have $\pmod 9$? Find an example of each.

$\phi(9) = 6$, so orders of integers $\pmod 9$ must be divisors of 6, i.e. 1, 2, 3, and 6. $1^1 \equiv 8^2 \equiv 4^3 \equiv 2^6 \equiv 1 \pmod 9$.

1.3

What is the smallest possible prime divisor of $2^{19} - 1$?

191.

1.4

Show that 3 is a primitive root of 7.

$$\begin{aligned}
\phi(7) &= 6 \\
3 &\equiv 3 \pmod 7 \\
3^2 &\equiv 2 \pmod 7 \\
3^3 &\equiv 6 \pmod 7 \\
3^4 &\equiv 4 \pmod 7 \\
3^5 &\equiv 5 \pmod 7 \\
3^6 &\equiv 1 \pmod 7
\end{aligned}$$

1.5

Find, by trial, a primitive root of 10.

3 is a primitive root of 10, as none of $3^1, 3^2, 3^3$ are $\equiv 1 \pmod{10}$, but $3^{\phi(10)} = 3^4 \equiv 1 \pmod{10}$.

1.6

Which of the integers 2, 3, ..., 25 do not have primitive roots?

8, 12, 15, 16, 20, 21, 24.

2 Problems

2.1

Find the orders of 1, 2, ..., 12 $\pmod{13}$.

1 (1), 12 (2), 3 (3), 6 (4), 4 (5), 12 (6), 12 (7), 4 (8), 3 (9), 6 (10), 12 (11), 2 (12).

2.2

Find the orders of 1, 2, ..., 16 $\pmod{17}$.

1 (1), 8 (2), 16 (3), 4 (4), 16 (5), 16 (6), 16 (7), 8 (8), 8 (9), 16 (10), 16 (11), 16 (12), 4 (13), 16 (14), 8 (15), 2 (16).

2.3

One of the primitive roots of 19 is 2. Find all of the others.

The numbers from 1 to 17 that are relatively prime to 18 are 1, 5, 7, 11, 13, 17. So, the other primitive roots of 19 are $2^5 \equiv 13, 2^7 \equiv 14, 2^{11} \equiv 15, 2^{13} \equiv 3, 2^{17} \equiv 10 \pmod{19}$.

2.4

One of the primitive roots of 23 is 5. Find all of the others.

The numbers from 1 to 22 that are relatively prime to 22 are 1, 3, 5, 7, 9, 13, 15, 17, 19, 21. So, the other primitive roots of 19 are $5^3 \equiv 10, 5^5 \equiv 20, 5^7 \equiv 17, 5^9 \equiv 11, 5^{13} \equiv 21, 5^{15} \equiv 19, 5^{17} \equiv 15, 5^{19} \equiv 7, 5^{21} \equiv 14 \pmod{23}$.

2.5

What are the orders of 2, 4, 7, 8, 11, 13, and 14 $\pmod{15}$? Does 15 have primitive roots?

4 (2), 2 (4), 4 (7), 4 (8), 2 (11), 4 (13), 2 (14). 15 does not have primitive roots.

2.6

What are the orders of 3, 7, 9, 11, 13, 17, and 19 $\pmod{20}$? Does 20 have primitive roots?

4 (3), 4 (7), 2 (9), 2 (11), 4 (13), 4 (17), 2 (19). 20 does not have primitive roots.

2.7

Which integers have order 6 $\pmod{31}$?

6, 26.

2.8

Which integers have order 6 $\pmod{37}$?

11, 27.

2.9

If $a, a \neq 1$, has order $t \pmod{p}$, show that

$$a^{t-1} + a^{t-2} + ... + 1 \equiv 0 \pmod{p}$$

Can write the sequence $a^{t-1} + a^{t-2} + ... + 1 = \frac{a^t - 1}{a-1}$. Since $(a-1, p) = 1$, can multiply both sides of a congruence with $\pmod{p}$ by $a-1$ to leave $a^t - 1$. Since by defintion $a^t \equiv 1 \pmod{p}$, then $a^t - 1 \equiv 0 \pmod{p}$.

2.10

If g and h are primitive roots of an odd prime p, then $g \equiv h^k \pmod{p}$ for some integer k. Show that k is odd.
Proved in the text that if h is a primitive root of p, then the least residue of h^k is a primitive root of p if and only if $(k, p-1) = 1$. Also know that $2|p-1$, since p is an odd prime. If also had $2|k$, then $(k, p-1)$ would be at least 2.

2.11

Show that if g and h are the primitive roots of an odd prime p, then the last residue of gh is not a primitive root of p.

Know that $g \equiv h^k \pmod{p}$ with an odd k from previous exercise. Then $gh \equiv h^{k+1} \pmod{p}$. Since $k+1$ and $p-1$ are both even, then $(k+1, p-1) \neq 1$, so gh cannot be a primitive root of p.

2.12

If g, h, and k are primitive roots of p, is the least residue of ghk always a primitive root of p?

Again write $g \equiv k^m$, $h \equiv k^n$, and $ghk \equiv k^{m+n+1}$, with $m+n+1$ odd.
Can one have $(m+n+1, p-1) \neq 1$?

2.13

Show that if a has order $3 \pmod{p}$, then $a+1$ has order $6 \pmod{p}$.

$a^3 - 1 = (a-1)(a^2+a+1) \equiv 0 \pmod{p}$. Notice that $(a+1)^3 = a^3 + 3a^2 + 3a + 1 \equiv 3(a^2+a+1) - 1 \equiv -1 \pmod{p}$. So $(a+1)^6 \equiv 1 \pmod{p}$. So, 6 must be a multiple of the order of $a+1$. We already showed it can't be 3. For 1, $a+1 \equiv 2 \pmod{p}$. For 2, $(a+1)^2 = a^2 + 2a + 1 = a^2 + a + 1 + a \equiv a \not\equiv 1 \pmod{p}$.

2.14

If p and q are odd primes and $q \mid a^p + 1$, show that either $q \mid a+1$ or $q = 2kp+1$ for some integer k.

If $q|a^p + 1$, can write $a^p \equiv -1 \pmod{q}$. This means that $a^{2p} \equiv 1 \pmod{q}$, and the order of a must divide $2p$. We can eliminate 1, because if $a \equiv 1 \pmod{q}$, then $a^p \equiv 1 \pmod{q}$, which was directly contradicted above. For the same reason, we can eliminate an order of p. So, a can have either an order of 2 or $2p$. If it's 2, then $a^2 \equiv 1 \pmod{q}$, so have $rq = a^2 - 1 = (a+1)(a-1)$. Since we know that $a \not\equiv 1 \pmod{q}$, that means $q|a+1$. If it is $2p$, then $2p|\phi(q)$, i.e. $2p|q-1$. Then $q = 2kp + 1$.

2.15

Suppose that a has order $4 \pmod{p}$. What is the least residue of $(a+1)^4 \pmod{p}$?

Know that $a^2 \equiv -1 \pmod{p}$ - can see this by writing $kp = (a^2+1)(a^2-1)$ and observing that $p \nmid a^2 - 1$ (or the order of a would be 2, not 4), so $p|a^2 - 1$. Expanding, $(a+1)^4 = a^4 + 4a^3 + 6a^2 + 4a^1 + 1 \equiv 1 - 4a - 6 + 4a + 1 \equiv -4 \pmod{p}$.

2.16

Show that $131071 = 2^{17} - 1$ is prime.

By the corollary from the text, any divisor of $2^p - 1$ must be of the form $2 * 17 * k + 1$. If 131071 is composite, it will have a divisor that is $\leq \sqrt{131071} \approx 360$. Furthermore, one of its divisors must be prime. That leaves us with candidates: 103, 137, 239, 307. None of these divides 131071.

2.17

Show that $(2^{19}+1)/3$ is prime.

By extension of the prompt of exercise 14, for a number to divide 2^p+1, it must either be equal to 3 or must have the form $2kp+1$. Presumably, we know 3 divides $3|2^{19}+1$ if we believe that $(2^{19}+1)/3 \in \mathbb{Z}$. That leaves us with candidates of the form $2*19*k+1 = 38*k+1$. By a similar logic as before, one of these must be of the form $3q$, where q is a prime.

2.18

If g is a primitive root of p, show that two consecutive powers of g have consecutive least residues. That is, show that there exists k such that $g^{k+1} \equiv g^k + 1 \pmod{p}$.

Rewrite the congruence as $g^k(g-1) \equiv 1 \pmod{p}$. Since g is a primitive root of p, there exists a k such that $g^k = x$ for any x in 1, 2, 3, ..., $p-1$. Also know that $g-1$ can only be $\equiv 0 \pmod{p}$ if $\phi(p) = p-1 = 1$, i.e. $p=2$, but 2 has no primitive roots, so we can exclude it. Furthermore, since $(g-1,p)=1$, we know that $x(g-1) \equiv 1 \pmod{p}$ must have exactly one solution, and that solution must be in $1, ..., p-1$.

2.19

If g is a primitive root of p, show that no three consecutive powers of g have consecutive least residues. That is, show that $g^{k+2} \equiv g^{k+1}+1 \equiv g^k+2 \pmod{p}$ is impossible for any k.

Notice that the last two parts of the congruence boil down to $g^k(g-1) \equiv 1 \pmod{p}$, as in the previous exercise. Now consider only the first and third parts of the congruence, $g^{k+2} \equiv g^k + 2 \pmod{p}$. This can be rewritten as $g^k(g^2-1) = g^k(g+1)(g-1) \equiv 2 \pmod{p}$. Since $g^k(g-1) \equiv 1 \pmod{p}$ must hold for the whole thing to hold, the last congruence would require $g+1 \equiv 2$, or $g \equiv 1 \pmod{p}$. But, since g is a primitive root of p, no power of g lesser than g^{p-1} is $\equiv 1 \pmod{p}$.

2.20

(a) Show that if m is a number having primitive roots, then the product of the positive integers less than or equal to m and relatively prime to it is congruent to -1 $\pmod{m}$.
(b) Show that the result in **(a)** is not always true if m does not have primitive roots.

(a) Know from the text that numbers with primitive roots must be of the form $1, 2, 4, p^e$, and $2p^e$.
For 1, the statement holds, because any digit +1 is divisible by 1.
For 2, the statement holds because $1 \equiv -1 \pmod{2}$.
For 4, the statement holds because $1*3 \equiv -1 \pmod{4}$.
For p, every integer from 1 to $p-1$ is relatively prime to p. We can thus write the product as $(p-1)!$, which we know from Wilson's Theorem is $\equiv -1 \pmod{p}$.
Now consider p^e with $e>1$. For even p, i.e. $p=2$, the product must consist of only odd integers, so adding 1 to whatever this product is will produce an even number. Now handle odd p. The product of the integers up to $p-1$ is the familiar $(p-1)!$. Then we have sequences of integers from $kp+1$ to $(k+1)p-1$. Notice that $\pmod{p}$, this is the same as a sequence of 1 to $p-1$. We have p^{e-1} such sequences, which we've shown are all individually $\equiv -1 \pmod{p}$. Since p odd, $p^{e-1} * -1 \equiv -1 \pmod{p}$.
For $2p$, the product of integers must exclude all even ones, and thus looks like $1*3*...*(p-1)*(p+2)*(p+4)*...*(2p-1)$. If you take the $p+2k$ terms $\pmod{p}$, these "fill in" the dropped even terms of the product up to p, so we're left with $(p-1) \equiv -1 \pmod{p}$.
For $2p^e$, the argument is the same as for p^e with odd p.
(b) The product for 8 is $1*3*5*7 = 105$, which is $\equiv 1 \pmod{8}$.