1. (§2.1, problem 34) Show that an integer $m > 1$ is a prime if and only if m divides $(m-1)! + 1$.

Proof: Suppose m is prime. Then by Wilson's theorem, $(m-1)! \equiv -1 \pmod{m}$. That is, m divides $(m-1)! + 1$.

Conversely, suppose $m > 1$ is composite. Then there is some prime $p < m$ such that $p|m$. Since $p \leq m-1$, p also divides $(m-1)!$, and thus

$$(m-1)! + 1 \equiv 0 + 1 \equiv 1 \pmod{p}.$$

This implies that $(m-1)! + 1 \not\equiv 0 \pmod{m}$, for if $(m-1)! + 1$ were congruent to 0 modulo m, it would be divisible by m, and therefore divisible by p. ∎

Alternate Proof: Suppose m is prime. Then by Wilson's theorem, $(m-1)! \equiv -1 \pmod{m}$. That is, m divides $(m-1)! + 1$.

Conversely, suppose $m > 1$ and m divides $(m-1)! + 1$. Then $(m-1)! + 1 \equiv 0 \pmod{m}$, so $(m-1)! \equiv -1 \pmod{m}$.

It follows by Theorem 2.4 that $((m-1)!, m) = (-1, m)$. Since the only positive divisor of -1 is 1, we have $(-1, m) = 1$, and so $((m-1)!, m) = 1$.

Now $(m-1)!$ is divisible by every positive integer less than m, so $((m-1)!, m) = 1$ implies that m has no divisors strictly between 1 and m. Thus m is prime. ∎

2. (§1.2, problem 32) Let $n \geq 2$ and k be any positive integers. Prove that $(n-1)^2 | (n^k - 1)$ if and only if $(n-1)|k$.

Proof: Write n^k as $((n-1)+1)^k$. Then by the Binomial theorem,

$$\begin{aligned} n^k &= \sum_{i=0}^{k} \binom{k}{i} (n-1)^i \\ &= 1 + k(n-1) + \sum_{i=2}^{k} \binom{k}{i} (n-1)^i \\ &= 1 + k(n-1) + (n-1)^2 \sum_{i=2}^{k} \binom{k}{i} (n-1)^{i-2}. \end{aligned}$$

Since every term in the last sum is an integer, we have shown that

$$n^k \equiv 1 + k(n-1) \pmod{(n-1)^2}$$

that is,

$$n^k - 1 \equiv k(n-1) \pmod{(n-1)^2}. \tag{1}$$

Now suppose $(n-1)|k$. Then $(n-1)^2|k(n-1)$, so $k(n-1) \equiv 0 \pmod{(n-1)^2}$, and it follows from (1) that $n^k - 1 \equiv 0 \pmod{(n-1)^2}$, that is, $(n-1)^2|n^k - 1$.

Conversely, if $(n-1)^2|n^k-1$, then from (1) we get that $k(n-1) \equiv 0 \pmod{(n-1)^2}$, so that $(n-1)^2|k(n-1)$. From this and the fact that $n-1 \neq 0$, it follows (by Theorem 1.1(6)) that $n-1|k$. ∎

Alternate proof: We have the factorization

$$(n^k - 1) = (n-1)(n^{k-1} + n^{k-2} + \cdots + n + 1),$$

so the problem is to prove that $n-1$ divides $(n^{k-1} + n^{k-2} + \cdots + n + 1)$ if and only if $n-1$ divides k.

Note that $n^j = ((n-1)+1)^j$ for every integer $j \geq 0$, so that

$$\begin{aligned} n^j &= \sum_{i=0}^{j} \binom{j}{i} (n-1)^i \\ &= 1 + (n-1)Z \end{aligned}$$

for some integer Z, and thus $n^j \equiv 1 \pmod{n-1}$ for every integer $j \geq 0$. This means that

$$\begin{aligned} (n^{k-1} + n^{k-2} + \cdots + n + 1) &\equiv 1 + 1 + \cdots + 1 + 1 \pmod{n-1} \\ &\equiv k \pmod{n-1}. \end{aligned}$$

Thus $n-1$ divides $n^{k-1} + n^{k-2} + \cdots + n + 1$ (and thus $(n-1)^2$ divides $n^k - 1$) if and only if $k \equiv 0 \pmod{n-1}$, that is, if and only if $(n-1)|k$. ∎

3. (Based on §2.1, problem 43) Let p be an odd prime. Show that $\{2, 4, 6, \ldots, 2(p-1)\}$ is a reduced residue system modulo p. Use this result to show that if p is an odd prime, then

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Proof: Let $S = \{2, 4, \ldots, 2(p-1)\}$. To show that S is a reduced residue system mod p, we verify that each element of S is relatively prime to p and that no element of S is

congruent to any other mod p. Since $|S| = p-1$, it will follow that we have a reduced residue system.

Consider $2a \in S$. If $(2a, p) \neq 1$, then $p|2a$, and since p is prime, it follows that $p|2$ or $p|a$. But $p > 2$ and $p > a$ as well, since $0 < a \leq p-1$. So $(2a, p) = 1$.

Now suppose $2a \equiv 2b \pmod{p}$. Then p divides $2a - 2b = 2(a-b)$. Since $p \not| 2$, it must be that $p|(a-b)$. But a and b are both from the set $\{1, 2, \ldots, p-1\}$, so $|a-b| < p$. Thus $p|(a-b)$ implies that $a - b = 0$, so $a = b$, and thus $2a = 2b$.

This completes the proof that S is a reduced residue system modulo p.

Since $\{1, 2, \ldots, p-1\}$ is another reduced residue system modulo p, we know that

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots 2(p-1) &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ &\equiv (p-1)! \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

by Wilson's theorem.

Thus we have

$$-1 \equiv (2 \cdot 4 \cdot 6 \cdots (p-1)) \cdot ((p+1) \cdot (p+3) \cdots 2(p-1)) \pmod{p}.$$

Multiplying the factors in pairs from the outside in, we get

$$\begin{aligned} -1 &\equiv (2(2p-2)) \cdot (4(2p-4)) \cdot (6(2p-6)) \cdots ((p-1)(2p-(p-1)) \pmod{p} \\ &\equiv (2(-2)) \cdot (4(-4)) \cdot (6(-6)) \cdots (p-1)(-(p-1)) \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left(2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2\right) \pmod{p} \end{aligned}$$

Multiplying both sides of the congruence above by $(-1)^{\frac{p-1}{2}}$, we get

$$\begin{aligned} 2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 &\equiv (-1)(-1)^{\frac{p-1}{2}} \pmod{p} \\ &\equiv (-1)^{\frac{p+1}{2}} \end{aligned}$$

as required. ∎

4. (§2.1, problem 54)

(a) Note that $341 = 11 \cdot 31$. Without using excessive computer power, show that $2^{341} \equiv 2 \pmod{341}$, but that $3^{341} \not\equiv 3 \pmod{341}$.

(b) Show that 561 is a pseudoprime to every base, even though 561 is not prime.

Solution:

(a) We need to show that $2^{341} \equiv 2$ modulo 11 and modulo 31. Because 11 is prime and $2 \not| 11$, we know that

$$2^{10} \equiv 1 \pmod{11},$$

from which it follows that

$$2^{341} \equiv (2^{10})^{34} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{11}.$$

Similarly, since 31 is prime and $2 \not| 31$, we know that

$$2^{30} \equiv 1 \pmod{31},$$

from which it follows that

$$2^{341} \equiv (2^{30})^{11} \cdot 2^{11} \equiv 2^{11} \pmod{31}.$$

Observing that $2^5 = 32 \equiv 1 \pmod{31}$, we conclude that $2^{10} \equiv 1 \pmod{31}$, so that

$$2^{11} \equiv 2 \pmod{31}.$$

This shows that $2^{341} \equiv 2 \pmod{31}$ and thus that $2^{341} \equiv 2 \pmod{341}$.
We now turn to base 3. Since $3 \not| 31$, we know $3^{30} \equiv 1 \pmod{31}$, so that

$$3^{341} \equiv (3^{30})^{11} \cdot 3^{11} \equiv 3^{11} \pmod{31}.$$

Next, with some light calculator use, we find the following congruences:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{31} \\ 3^2 &\equiv 9 \pmod{31} \\ 3^4 &\equiv 19 \pmod{31} \\ 3^8 &\equiv 20 \pmod{31}. \end{aligned}$$

Thus $3^{11} \equiv 3^8 \cdot 3^4 \cdot 3^1 \equiv 20 \cdot 9 \cdot 3 \equiv 13 \pmod{31}$.
We conclude that $3^{341} \not\equiv 3 \pmod{341}$, for if it were, then we would have $3^{341} \equiv 3^{11} \equiv 3 \pmod{31}$, and this is not the case.

(b) We need to show that a^{561} is congruent to a modulo 3, modulo 11, and modulo 17, for every integer a.

Working first modulo 3, we have by Fermat that

$$a^2 \equiv 1 \pmod 3$$

if $3 \nmid a$. Thus

$$\begin{aligned} a^{561} &\equiv (a^2)^{280} \cdot a \pmod 3 \\ &\equiv a \pmod 3. \end{aligned}$$

If $3|a$, then $a^{561} \equiv a \equiv 0 \pmod 3$.

Working modulo 11, we know that if $11 \nmid a$, then

$$a^{10} \equiv 1 \pmod{11}$$

so that

$$\begin{aligned} a^{561} &\equiv (a^{10})^{56} \cdot a \pmod{11} \\ &\equiv a \pmod{11}. \end{aligned}$$

Again, if $11|a$, then $a^{561} \equiv a \equiv 0 \pmod{11}$.

Finally, working modulo 17, we find that for $17 \nmid a$,

$$a^{16} \equiv 1 \pmod{17}$$

so that

$$\begin{aligned} a^{561} &\equiv (a^{16})^{35} \cdot a \pmod{17} \\ &\equiv a \pmod{17}. \end{aligned}$$

If $17|a$, then $a^{561} \equiv a \equiv 0 \pmod{17}$.

Since $a^{561} - a$ is divisible by 3, 11, and 17, it must be divisible by their least common multiple, 561.