The art of doing mathematics consists in finding that special case which contains all the germs of generality. - David Hilbert.

Question 1. Fermat's little theorem says that if p is prime and $\gcd(2,p)=1$, then $2^{p-1}\equiv 1 \bmod p$. However, the converse is not true: if m is a number, $\gcd(2,m)=1$, and $2^{m-1}\equiv 1 \bmod m$, this **does not imply** that m is a prime number. A number m is called a 2-pseudoprime if (a) m is composite, and (b) $2^{m-1}\equiv 1 \bmod m$. Show that 341 is a 2-pseudoprime, i.e., show that $2^{340}\equiv 1 \bmod 341$, but 341 is a composite number.

Solution:
The number 341 is a 2-pseudoprime is 341 is composite and $2^{340}\equiv 1 \mod 341$. First, let us factor 341. Clearly, $341 < 19^2$ therefore $\sqrt{341} < 19$. Thus, 341 must have a prime divisor less than 19. The divisibility test for 11 shows that $341 \equiv 3+4-1 \equiv 0 \mod 11$, so it is divisible by 11. Thus $341 = 11\cdot 31$.

Now we calculate $2^340 \mod 341$. We can calculate:

$$\phi(341)=\phi(11)\phi(31)=300$$

thus, by Euler's theorem $2^{300}\equiv 1 \mod 341$ and

$$2^{340}\equiv 2^{300}\cdot 2^{40}\equiv 2^{40} \mod 341.$$

Finally, since $40 = 32+8$, we calculate some powers of 2:

$$2, 2^2\equiv 4, 2^4\equiv 16, 2^8\equiv 256, 2^{16}\equiv 64, 2^{32}\equiv 4 \mod 341$$

Hence:

$$2^{340}\equiv 2^{40}\equiv 2^{32}\cdot 2^8\equiv 4\cdot 256\equiv 1 \mod 341.$$

Question 2.

(a) Verify that if n is composite, i.e., $n=ab$, then the polynomial x^n-1 factors as

$$x^n-1=(x^b-1)(x^{b(a-1)}+x^{b(a-2)}+\cdots+x^b+1).$$

(b) Show that if n is composite, then $m=2^n-1$ is also composite.

(c) Show that if n is a 2-pseudoprime, then $m=2^n-1$ is also a 2-pseudoprime.

(d) Use part (c) to show that there are infinitely many 2-pseudoprimes.

Solution:

1. Simply multiplying the polynomials proves the identity. Otherwise, note that $x^a-1=(x-1)(x^{a-1}+\cdots+x+1)$ and substitute x by x^b.

2. By the previous identity, if $n=ab$, with $1<a,b<n$, then

$$m=2^n-1=2^{ab}-1=(2^b-1)(2^{b(a-1)}+2^{b(a-2)}+\cdots+2^b+1).$$

Since $a,b>1$, both factors are >1, and therefore $m=2^n-1$ is composite.

3. Suppose n is a 2-pseudoprime. Then, n is composite and $2^{n-1} \equiv 1 \bmod n$. By the previous part, $m = 2^n - 1$ is composite as well, so we only need to show that $2^{m-1} \equiv 1 \bmod m$. Since $2^{n-1} \equiv 1 \bmod n$, this implies that there is some $k \geq 1$ such that $2^{n-1} - 1 = nk$. Now,

$$2^{m-1} \equiv 2^{(2^n-1)-1} \equiv 2^{2^n-2} \equiv 2^{2(2^{n-1}-1)} \equiv 2^{2nk} \equiv (2^n)^{2k} \equiv 1^{2k} \equiv 1 \bmod (2^n - 1),$$

where we have used the fact that $2^n \equiv 1 \bmod (2^n - 1)$. Thus, $2^{m-1} \equiv 1 \bmod m$, and m is composite, and this shows that m is a 2-pseudoprime.

4. We just showed that if n passes the 2-pseudoprime test then $2^n - 1$ does also. Moreover, if n is composite then $2^n - 1$ is composite. Thus, let n be a 2-pseudoprime (such as 341), so that n is composite and it passes the 2-pseudoprime test. Then $2^n - 1$ is composite and it passes the 2-pseudoprime test, and therefore it is a 2-pseudoprime. Hence, the numbers in the sequence:

$$A_0 = 341, \quad A_{n+1} = 2^{A_n} - 1$$

are infinitely many 2-pseudoprimes.

Question 3. A Carmichael number is a composite positive integer m such that $b^{m-1} \equiv 1 \bmod m$ for all integers b which are relatively prime to m.

(a) Show that 561 is a 2-pseudoprime and a 5-pseudoprime, i.e., show that

$$2^{560} \equiv 1 \bmod 561, \quad \text{and} \quad 5^{560} \equiv 1 \bmod 561.$$

(b) Show that $b^{80} \equiv 1 \bmod 561$, for all b relatively prime to 561. (Hint: Use Fermat's little theorem.)

(c) Use part (b) to conclude that 561 is a Carmichael number. (In fact, 561 is the smallest Carmichael number.)

(d) Prove that 1105 is also a Carmichael number. (1105 is the second Carmichael number.)

Solution:

1. The number $561 = 3 \cdot 11 \cdot 17$ is composite. Moreover, $2^2 \equiv 5^2 \equiv 1 \bmod 3$, $2^{10} \equiv 5^{10} \equiv 1 \bmod 11$, and $2^{16} \equiv 5^{16} \equiv 1 \bmod 17$, by Fermat's little theorem. In particular, $2^{80} \equiv 5^{80} \equiv 1 \bmod 3$, 11 and 17, because 2, 10 and 16 are divisors of 80. Thus, by the Chinese remainder theorem, $2^{80} \equiv 1 \bmod 561$. Since $560 = 80 \cdot 7$ it follows that

$$2^{560} \equiv (2^{80})^7 \equiv 1^7 \equiv 1 \bmod 561,$$

and similarly $5^{560} \equiv 1 \bmod 561$. Hence, the number 561 is a 2-pseudoprime and also a 5-pseudoprime.

2. If b is relatively prime to $561 = 3 \cdot 11 \cdot 17$, it follows from Fermat's little theorem that $b^2 \equiv 1 \bmod 3$, $b^{10} \equiv 1 \bmod 11$, and $b^{16} \equiv 1 \bmod 17$. In particular, $b^{80} \equiv 1 \bmod 3$, 11 and 17, because 2, 10 and 16 are divisors of 80. Thus, by the Chinese remainder theorem, $b^{80} \equiv 1 \bmod 561$.

3. Hence, 561 is a Carmichael number, because it is composite and $b^{560} \equiv (b^{80})^7 \equiv 1 \bmod 561$ for all b relatively prime to 561.
4. Similarly, $1105 = 5 \cdot 13 \cdot 17$ is composite. If b is relatively prime to 1105, then it follows from Fermat's little theorem that $b^4 \equiv 1 \bmod 5$, $b^{12} \equiv 1 \bmod 13$, and $b^{16} \equiv 1 \bmod 17$. In particular, $b^{48} \equiv 1 \bmod 5$, 13 and 17, because 4, 12 and 16 are divisors of 48. Thus, by the Chinese remainder theorem, $b^{48} \equiv 1 \bmod 1105$. Finally, since $1104 = 48 \cdot 23$, it follows that
$$b^{1104} \equiv (b^{48})^{23} \equiv 1 \bmod 1105$$
for all b relatively prime to 1105. Hence, 1105 is also a Carmichael number.

Question 4. Show that for any prime p the polynomial $x^p - x$ factors as

$$x(x-1)(x-2)\cdots(x-(p-1))$$

over $(\mathbb{Z}/p\mathbb{Z})[x]$. Check that this works for $p = 5$.

Solution:
Let $f(x) = x^5 - x$. Recall that by the root theorem, if $f(a \bmod 5) \equiv 0 \bmod 5$ then $(x - a)$ divides $f(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$. Moreover, by Fermat's little theorem, we know that $a^5 \equiv a \bmod 5$, for all $a \equiv 0, 1, 2, 3, 4 \bmod 5$. Therefore, $a \equiv 0, 1, 2, 3, 4 \bmod 5$ are all roots of $x^5 - x$ and, hence, $(x - a)$ divides $x^5 - x$ for $a = 0, 1, 2, 3, 4$, in $\mathbb{Z}/5\mathbb{Z}[x]$. Since $(x-0)(x-1)(x-2)(x-3)(x-4)$ is a monic polynomial of degree 5 that divides $x^5 - x$, they must be equal. Hence:

$$x^5 - x \equiv x(x-1)(x-2)(x-3)(x-4) \bmod 5.$$

Let now $f(x) = x^p - x$. Recall that by the root theorem, if $f(a \bmod p) \equiv 0 \bmod p$ then $(x - a)$ divides $f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Moreover, by Fermat's little theorem, we know that $a^5 \equiv a \bmod p$, for all $a \equiv 0, 1, 2, \ldots, p-1 \bmod p$. Therefore, $a \equiv 0, 1, 2, \ldots, p-1 \bmod p$ are all roots of $x^p - x$ and, hence, $(x - a)$ divides $x^p - x$ for $a = 0, 1, 2, \ldots, p-1$, in $\mathbb{Z}/p\mathbb{Z}[x]$. Since $(x-0)(x-1)(x-2)\cdots(x-(p-1))$ is a monic polynomial of degree p that divides $x^p - x$, they must be equal. Hence:

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-(p-1)) \bmod p.$$

Question 5. Prove that 74 is a primitive root modulo 89.

Solution:
First we show that 2 has order 11 modulo 89. Notice that if we show that $2^{11} \equiv 1 \bmod 89$, then the order must be 11 because the order would divide 11 and it is clearly not just 1, so it must be 11. In order to show that $2^{11} \equiv 1 \bmod 89$, notice that

$$2^6 \equiv 64 \equiv -25 \equiv -(5^2) \bmod 89.$$

Moreover $5^4 \equiv (25^2) \equiv 625 \equiv 2 \bmod 89$. Therefore:

$$2^{12} \equiv (2^6)^2 \equiv (-5^2)^2 \equiv 5^4 \equiv 2 \bmod 89$$

and so, $2^{11} \equiv 1 \bmod 89$.

Next we show that 37 has order 8 modulo 89. Calculate $37^2 \equiv 34 \bmod 89$ and $34^2 \equiv 88 \equiv -1 \bmod 89$. Therefore $37^8 \equiv (37^4)^2 \equiv (-1)^2 \equiv 1 \bmod 89$.

Finally, since $\mathrm{ord}(2) = 11$, $\mathrm{ord}(37) = 8$ and $(11, 8) = 1$, it follows that $\mathrm{ord}(74) = \mathrm{ord}(2 \cdot 37) = 11 \cdot 8 = 88 = 89 - 1$. Hence, 74 is a primitive root modulo 89.

Question 6. Find a primitive root modulo 61.

Solution:
Let us check that 2 is a primitive root modulo 61. Thus, we need to check that the order of 2 is exactly 60. Notice that the order of 2 must be a divisor of $60 = 4 \cdot 3 \cdot 5$, so the possible orders are: $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$. We need to check that $2^d \not\equiv 1 \bmod 61$ for all $d = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ but $2^{60} \equiv 1 \bmod 61$ (the last congruence is, of course, a result of Fermat's little theorem and it doesn't need to be checked).

$$
\begin{aligned}
2 &\not\equiv 1 \bmod 61,\\
2^2 &\equiv 4 \not\equiv 1 \bmod 61,\\
2^3 &\equiv 8 \not\equiv 1 \bmod 61,\\
2^4 &\equiv 16 \not\equiv 1 \bmod 61,\\
2^5 &\equiv 32 \not\equiv 1 \bmod 61,\\
2^6 &\equiv 64 \equiv 3 \not\equiv 1 \bmod 61,\\
2^{10} &\equiv 2^6 \cdot 2^4 \equiv 3 \cdot 16 \equiv 48 \not\equiv 1 \bmod 61,\\
2^{12} &\equiv 2^{10} \cdot 2^2 \equiv 48 \cdot 4 \equiv 192 \equiv 9 \not\equiv 1 \bmod 61,\\
2^{15} &\equiv 2^{12} \cdot 2^3 \equiv 9 \cdot 8 \equiv 11 \not\equiv 1 \bmod 61,\\
2^{20} &\equiv 2^{15} \cdot 2^5 \equiv 11 \cdot 32 \equiv 352 \equiv 47 \not\equiv 1 \bmod 61,\\
2^{30} &\equiv (2^{15})^2 \equiv 11^2 \equiv 121 \equiv -1 \not\equiv 1 \bmod 61,\\
2^{60} &\equiv (2^{30})^2 \equiv (-1)^2 \equiv 1 \bmod 61.
\end{aligned}
$$

Question 7. Find a primitive root modulo 73.

Solution:
We begin by calculating the order of 2 modulo 73. Notice that the possible orders are the divisors of $72 = 2^3 \cdot 3^2$, which are: $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$. After some calculations, we find that $2^9 \equiv 1 \bmod 73$ and not before. Thus, the order of 2 is 9, not a primitive root.

Let us try 3 next. After the appropriate calculations, we find that $3^{12} \equiv 1 \bmod 73$ and not before. Therefore the order is 12. Since $(12, 9) = 3$, we use 3 to find another congruence of order 4. Since 3 has order 12 then $3^3 = 27$ must have order 4. Now, if we had instead an element a of order 8, then we would be almost done because $2a$ would have order $8 \cdot 9 = 72$. Since 27 has order 4, if we have a such that $a^2 \equiv 27$ then a would have order 8. So we try to find a root of $x^2 \equiv 27 \bmod 73$. It turns out that $10^2 \equiv 27 \bmod 73$. And we can check that the order of 10 is precisely 8 modulo 73.

Since 8 and 9 are relatively prime, and $\mathrm{ord}(2) = 9$, $\mathrm{ord}(10) = 8$, it turns out that $\mathrm{ord}(20) = \mathrm{ord}(2 \cdot 10) = 8 \cdot 9 = 72$, by a result in class. Therefore, 20 is a primitive root modulo 73.

Question 8. Let p be an odd prime. Show that if b is a primitive root modulo p then

$$b^{(p-1)/2} \equiv -1 \mod p.$$

Solution:
Let p be an odd prime, let b be a primitive root modulo p, notice that $(p-1)/2$ is an integer (because p is odd) and put

$$a \equiv b^{(p-1)/2} \bmod p.$$

First, we claim that $a^2 \equiv 1 \bmod p$. Indeed:

$$a^2 \equiv (b^{(p-1)/2})^2 \equiv b^{p-1} \equiv 1 \bmod p$$

by Fermat's little theorem. However, we know that $x^2 \equiv 1 \bmod p$ has only two solutions, namely ± 1. But since b is a primitive root, we cannot have $b^{(p-1)/2} \equiv 1 \bmod p$ because this would contradict the fact that the order of b is precisely $p-1$. Therefore, $a \equiv b^{(p-1)/2} \equiv -1 \bmod p$ as claimed.

Question 9. Prove Wilson's theorem using the fact that there exists a primitive root modulo p. (Hint: suppose that g is a primitive root mod p, and write every unit as a power of g.)

Solution:
Let p be an odd prime and let b be a primitive root modulo p. Then the order of b is precisely $p-1$ and, therefore, every unit $1, 2, \ldots, p-1$ modulo p can be expressed as one of the powers:

$$b, b^2, b^3, \ldots, b^{p-1} \bmod p.$$

Therefore, $\{1, 2, \ldots, p-1\}$ and $\{b, b^2, \ldots, b^{p-1}\}$ are both complete systems of representatives of the units modulo p and so:

$$(p-1)! \equiv 1 \cdot 2 \cdots (p-1) \equiv b \cdot b^2 \cdots b^{p-1} \equiv b^{1+2+\cdots+(p-1)} \equiv b^{p(p-1)/2} \equiv (b^{(p-1)/2})^p \equiv (-1)^p \equiv -1$$

modulo p, where we have used the previous problem (i.e., $b^{(p-1)/2} \equiv -1 \bmod p$ when b is a primitive root modulo p) and the equality $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

Alternatively, let p be an odd prime, and let b be a primitive root modulo p. Then:

$$\begin{aligned}
(p-1)! &\equiv b \cdot b^2 \cdots b^{p-1} \\
&\equiv (b \cdot b^{p-1})(b^2 \cdot b^{p-2}) \cdots (b^{(p-1)/2} \cdot b^{(p+1)/2}) \\
&\equiv b^p \cdot b^p \cdots b^p \\
&\equiv b \cdot b \cdots b \\
&\equiv b^{(p-1)/2} \equiv -1 \bmod p,
\end{aligned}$$

where we have used Fermat's little theorem to show that $b^p \equiv b \bmod p$ (or the fact that the order of b is $p-1$), and the solution of the previous problem (i.e., $b^{(p-1)/2} \equiv -1 \bmod p$ when b is a primitive root modulo p).