Example 112. Show that 561 is an absolute pseudoprime.

Solution. We need to show that $a^{560} \equiv 1 \pmod{561}$ for all invertible residues modulo 561.

Since $561 = 3 \cdot 11 \cdot 17$, $a^{560} \equiv 1 \pmod{561}$ is eqivalent to $a^{560} \equiv 1 \pmod{p}$ for all of $p = 3, 11, 17$.

By Fermat's little theorem, we have $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$. Since $2, 10, 16$ all divide 560, it follows that indeed $a^{560} \equiv 1 \pmod{p}$ for $p = 3, 11, 17$.

Comment. Korselt's criterion (1899) states that what we just observed in fact characterizes absolute pseudoprimes. Namely, a composite number n is an absolute pseudoprime if and only if n is square-free, and for all primes p dividing n, we also have $p - 1 | n - 1$.

Theorem 113. (Korselt's Criterion) Let n be positive and composite. Then $a^n \equiv a \pmod{n}$ holds for any integer a if and only if n is squarefree and $(p-1)|(n-1)$ for any prime divisor p of n.

[if and only if $a^{n-1} \equiv 1 \pmod{n}$ holds for any integer a with $\gcd(a, n) = 1$]

Proof. Here, we will only the "if" part (the "only if" part is also not hard to show but the typical proof requires a little more insight into primitive roots than we currently have). In other words, assume that n is **squarefree** and $(p-1)|(n-1)$ for any prime divisor p of n. Let a be any integer. We will show that $a^n \equiv a \pmod{n}$.

n being squarefree means that its prime factorization is of the form $n = p_1 \cdot p_2 \cdots p_d$ for distinct primes p_i (this is equivalent to saying that there is no integer $m > 1$ such that $m^2 | n$). By Fermat's little theorem $a^{p_i - 1} \equiv 1 \pmod{p_i}$ and, since $(p_i - 1)|(n-1)$, $a^{n-1} \equiv 1 \pmod{p_i}$. But, wait! This is only true if $\gcd(a, p_i) = 1$, that is, $a \not\equiv 0 \pmod{p_i}$. However, in either case (that is, for all a), we get $a^n \equiv a \pmod{p_i}$.

It then follows by the Chinese remainder theorem that $a^n \equiv a \pmod{n}$. □

15 Multiplicative order and primitive roots

Example 114. (warmup) Compute the powers of 2 modulo 11.

Solution. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3, 2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$, and now the numbers we get will repeat...

Note. By **Fermat's little theorem**, it was clear from the beginning that $2^{10} \equiv 1 \pmod{11}$. Our computation shows that $k = 10$ is the smallest exponent such that $2^k \equiv 1 \pmod{11}$. We therefore say that 2 has **multiplicative order** 10 modulo 11.

Also notice that the values 2^0, 2^1, ..., 2^9, together with 0, form a complete set of residues modulo 11. For that reason, we say that 2 is a **primitive root** modulo 11.

Definition 115. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Definition 116. If the multiplicative order of an residue a modulo n equals $\phi(n)$ [in other words, the order is as large as possible], then a is said to be **primitive root** modulo n.

A primitive root is also referred to as a **multiplicative generator** (because the products of a, that is, $1, a$, $a^2, a^3, \ldots$, produce all [$\phi(n)$ many] invertible residues).

Armin Straub
straub@southalabama.edu

Example 117. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod 7$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
- $2 \pmod 9$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Advanced comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.