Fermat's little theorem

Fermat's little theorem, a famous theorem from elementary number theory, will be explored in this lab. Let p be a prime and a any positive integer that is not divisible by p. Then Fermat's little theorem states that

$$a^{p-1} \equiv 1 \mod p.$$

Fermat's little theorem is the foundation for many results in number theory and is the basis for several factorization methods in use today.

Exercises

1. Use the ring structure of $\mathbb{Z}_p$ and the software PascGaloisJE or one of the supporting Java applets to verify Fermat's little theorem for several different primes p and positive integers a which are relatively prime to p.

2. Why does a have to be relatively prime to p? What happens if $\gcd(a, p) = p$? Give some examples.

3. Is $p - 1$ necessarily the *smallest* positive integer r such that $a^r \equiv 1 \mod p$? Why or why not?

4. Use Fermat's little theorem to solve the following linear congruences.

   (a) $5x \equiv 14 \mod 11$

   (b) $6x \equiv 10 \mod 23$

5. Use Fermat's little theorem to evaluate $2^{235} \mod 19$.

6. Use Lagrange's theorem from group theory to prove Fermat's little theorem.

7. In some texts, Fermat's little theorem is stated as $a^p \equiv a \mod p$ for any integer a. Use the binomial theorem and induction on a to prove this version of Fermat's little theorem for $a \geq 0$. (*Hint*: $(x + y)^p = x^p + y^p \mod p$.) Use this result to prove Fermat's little theorem for $a < 0$.

8. Is the statement $a^n \equiv a \mod n$ true if n is a composite number? Use the software PascGaloisJE or one of the supporting Java applets to explore this question. (If you get stuck, try $n = 341$ and $a = 2$.)