Exercises 8

Exercises

1. Prove that
$$3^{512} \equiv 1 \pmod{1024}.$$
2. Find the remainder when 7^{51} is divided by 144.
3. Find the remainder when 2^{10^8} is divided by 31.
4. Compute the order of 2 with respect to the prime moduli 3, 5, 7, 11, 13, 17, and 19.
5. Compute the order of 10 with respect to the modulus 7.
6. Let r_i denote the least nonnegative residue of $10^i \pmod 7$. Compute r_i for $i = 1, \ldots, 6$. Compute the decimal expansion of the fraction $1/7$ without using a calculator. Can you find where the numbers $r_1, \ldots, r_6$ appear in the process of dividing 7 into 1?
7. Compute the order of 10 modulo 13. Compute the period of the fraction $1/13$.
8. Let p be prime and a an integer not divisible by p. Prove that if $a^{2^n} \equiv -1 \pmod p$, then a has order 2^{n+1} modulo p.
9. Let m be a positive integer not divisible by 2 or 5. Prove that the decimal expansion of the fraction $1/m$ is periodic with period equal to the order of 10 modulo m.
10. Prove that the decimal expansion of $1/m$ is finite if and only if the prime divisors of m are 2 and 5.
11. Prove that 10 has order 22 modulo 23. Deduce that the decimal expansion of $1/23$ has period 22.
12. Prove that if p is a prime number congruent to 1 modulo 4, then there exists an integer x such that $x^2 \equiv -1 \pmod p$.

    Hint: Observe that
$$\begin{aligned}(p-1)! &\equiv \prod_{j=1}^{(p-1)/2} j(p-j) \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \\ &\equiv (-1)^{(p-1)/2} \left(\prod_{j=1}^{(p-1)/2} j \right)^2 \pmod p,\end{aligned}$$
    and apply Theorem 2.4.
13. Prove that if $n \geq 2$, then $2^n - 1$ is not divisible by n.

    Hint: Let p be the smallest prime that divides n. Consider the congruence $2^n \equiv 1 \pmod p$.
14. Prove that if p and q are distinct primes, then
$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$
15. Prove that if m and n are relatively prime positive integers, then
$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$
16. Let p be an odd prime. By Euler's theorem, if $(a, p) = 1$, then
$$f_p(a) = \frac{a^{p-1} - 1}{p} \in \mathbf{Z}.$$
    Prove that if $(ab, p) = 1$, then
$$f_p(ab) \equiv f_p(a) + f_p(b) \pmod p.$$
17. Let $f(x)$ and $g(x)$ be polynomials with integer coefficients. We say that $f(x)$ is equivalent to $g(x)$ modulo p if
$$f(a) \equiv g(a) \pmod p \quad \text{for all integers } a.$$
    Prove that the polynomials x^9+5x^7+3 and $x^3-2x+24$ are equivalent modulo 7. Prove that every polynomial is equivalent modulo p to a polynomial of degree at most $p-1$.

    Hint: Use Fermat's theorem.