

Exercises 11

1. Find all cubic residues modulo 19.
2. Find all solutions of the congruence $x^3 \equiv 8 \pmod{19}$.
3. Define the map $f : (\mathbf{Z}/19\mathbf{Z})^\times \rightarrow (\mathbf{Z}/19\mathbf{Z})^\times$ by $f(x + 19\mathbf{Z}) = x^3 + 19\mathbf{Z}$. Prove that f is a homomorphism of the multiplicative group $(\mathbf{Z}/19\mathbf{Z})^\times$, and compute its kernel.
4. Find all fifth power residues modulo 11.
5. Find all sixth power residues modulo 11.
6. Define the map $f : (\mathbf{Z}/23\mathbf{Z})^\times \rightarrow (\mathbf{Z}/23\mathbf{Z})^\times$ by $f(x + 23\mathbf{Z}) = x^3 + 23\mathbf{Z}$. Prove that f is an isomorphism of the multiplicative group $(\mathbf{Z}/23\mathbf{Z})^\times$, that is, prove that f is a homomorphism that is one-to-one and onto.
7. Let x_a be the least nonnegative integer such that $x_a^3 \equiv a \pmod{11}$. Compute x_a for $a = 1, 2, \dots, 10$.
8. Prove that if $p \equiv 2 \pmod{3}$, then every integer not divisible by p is a cubic residue modulo p .
9. Prove that if $p \equiv 1 \pmod{6}$, then the product of the $(p-1)/3$ cubic residues modulo p is congruent to -1 modulo p .