CS5610: Computational Number Theory
Practice Problems

Due: 14/11/25

Attempt AT LEAST FOUR of these problems for HW3.

1. Let n be a product of distinct odd primes. Suppose that for every prime divisor p of n, it is the case that p divides $(n-p)$. Show that $a^{n-1} \equiv 1 \pmod{n}$ for every $a \in \mathbb{Z}_n^*$. Such numbers are called Carmichael numbers. Deduce that 561 is a Carmichael number.

2. Suppose that G is a finite group with identity e; let $a \in G$ and $a^d = e$. Show that $ord(a)$ must divide d.

3. Let p be an odd prime and $r \in \{1, 2, \ldots, p-1\}$. Show that there is a positive integer n such that $n^n - r$ is divisible by p.

4. Find $f(x) \in \mathbb{Z}_7[x]$ such that $f(x)(2x+1) \equiv 1 \bmod (x^2+1)$.

5. Let $n = 15$ and let $f(x) \in \mathbb{Z}_n[x]$ be a non-zero polynomial of degree 3 with exactly d distinct roots. What are the possible values of d?

6. Let p be an odd prime larger than 3. Show that $x^2 \equiv 3 \bmod p$ has a solution if and only if $p \equiv \pm 1 \bmod 12$.

7. Let p be an odd prime and let $f(x) = x^p - x - a \in \mathbb{Z}_p[x]$, where $a \neq 0 \in \mathbb{Z}_p$. Show that $f(x)$ is irreducible.

8. Let p be an odd prime and let $n = 2p+1$. Suppose that $2^p \equiv 1 \pmod{n}$. Show that n is prime.

9. Suppose that we modify the quadratic sieve algorithm in the following way: instead of computing factors of $b^2 - n$, we compute factors of $b^3 - n$ for $b \geq \lceil \sqrt[3]{n} \rceil$ and try find a relation of the form $\alpha^3 \equiv \beta^3 \pmod{n}$.

   (a) Explain what modifications should be made to the algorithm to find such α, β, and how to subsequently find factors of n.

   (b) For which values of n can this modified idea still work to find a factor and for which values of n will this modification never produce any factors?