Math 116 Spring 2022
Homework 4

Due Friday, April 29nd

Problem 1. (2.26) Let $\mathbb{F}_p$ be a finite field and let $N \mid p-1$. Prove that $\mathbb{F}_p^\times$ has an element of order N. This is true in particular for any prime power that divides $p-1$. (Hint. Use the fact that $\mathbb{F}_p$ has a primitive root.)

Problem 2. (2.28(a)–(c), with Sage) Use the Pohlig–Hellman algorithm (Theorem 2.31) to solve the discrete logarithm problem $g^x = a$ in $\mathbb{F}_p$ in each of the following cases

(a) $p = 433$, $g = 7$, $a = 166$.

(b) $p = 746497$, $g = 10$, $a = 243278$.

(c) $p = 41022299$, $g = 2$, $a = 39183497$. (Hint. $p = 2 \cdot 29^5 + 1$.)

Problem 3. (3.2) This exercise investigates what happens if we drop the assumption that $\gcd(e, p-1) = 1$ in Proposition 3.2. So let p be a prime, let $c \not\equiv 0 \pmod{p}$, let $e \geq 1$.

(a) Prove that if $x^e \equiv c \pmod{p}$ has one solution, then it has exactly $\gcd(e, p-1)$ distinct solutions. (Hint. Use the primitive root theorem combined with the extended Euclidean algorithm.)

(b) For how many non-zero values of $c \pmod{p}$ does $x^e \equiv c \pmod{p}$ have a solution?

Problem 4. (3.7, with Sage) Alice publishes her RSA public key: modulus $N = 2038667$ and exponent $e = 103$.

(a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?

(b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

Problem 5. (3.15, with Sage) Use the Miller–Rabin test on each of the following numbers. In each case, either provide a Miller–Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that are not Miller–Rabin witnesses for n.

(a) $n = 294409$

(b) $n = 294439$

(c) $n = 118901509$

(d) $n = 118901521$

Problem 6. (3.16) Suppose for a given RSA public key $N = pq$ Eve knows a pair e and d such that $2 \leq e, d < N - 1$ and $(x^e)^d \equiv x \pmod{N}$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

(a) Describe an analogue of the Miller–Rabin algorithm that can be used to search for nontrivial solutions to $t^2 \equiv 1 \pmod{N}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ (the "trivial" solutions are $t = \pm 1$).

(b) Suppose a is a nontrivial solution to $t^2 \equiv 1 \pmod{N}$. Show that $\gcd(a - 1, N)$ is one of the prime factors of N.