4400-001 - SPRING 2022 - WEEK 7 (2/22, 2/24)
PRIMITIVE ROOTS AND SOME BIG PRIMES

Some of these exercises can be found in Savin - Chapters 4 and 5.

Exercise 1 (required). Finding roots. The decryption method for RSA depended on:

Theorem. *If* $\gcd(e, \phi(m)) = 1$*, then for any* $a \in (\mathbb{Z}/m\mathbb{Z})^\times$*,*

$$x^e = a \mod m$$

has a unique solution given by $x = a^d$ *where* d *is the multiplicative inverse for* e *modulo* $\phi(m)$*.*

We quickly justified this statement in the lecture for Thursday last week, and you can find the proof written down (for an arbitrary finite group instead of $(\mathbb{Z}/m\mathbb{Z})^\times$) in Savin, Proposition 19 on p.68. Use this theorem to solve the following congruences:

(1) $x^5 \equiv 2 \mod 35$
(2) $x^{11} \equiv 13 \mod 35$
(3) $x^7 \equiv 11 \mod 63$
(4) $x^5 \equiv 3 \mod 64$
(5) **Optional - not to turn in**: For RSA we actually used a slightly stronger statement for special values of m: If $m = p_1 p_2 \dots p_k$ is a product of distinct prime numbers, then for $\gcd(e, \phi(m)) = 1$ and d the multiplicative inverse of $e \mod \phi(m)$, a^d is the unique solution to $x^e = a$ for *any* $a \in \mathbb{Z}/m\mathbb{Z}$ (i.e. a does not have to be in $(\mathbb{Z}/m\mathbb{Z})^\times$). Justify this statement using the Chinese Remainder Theorem. Is this true if m is not a product of distinct primes?

Exercise 2 (required). Primitive roots, orders of elements, and discrete logarithm

(1) Compute the orders of all elements in $\mathbb{F}_{13}^\times$. Which ones are primitive roots for $\mathbb{F}_{13}$ (i.e. have order 12)?
(2) Use the discrete logarithm modulo 11 with base 2 to solve the following congruences:
   (a) $7x \equiv 6 \mod 11$
   (b) $5x \equiv 3 \mod 11$
   (c) $4x^2 \equiv 9 \mod 11$
(3) The number 2 is a primitive root modulo 19. Compute the powers $2^k \mod 19$ for $k = 0, 1, 2 \dots, 18$ to obtain a table for the discrete logarithm with base 2 in $\mathbb{F}_{19}$. Then use this to solve the equation

$$x^5 \equiv 7 \mod 19.$$

Exercise 3. The Lucas-Lehmer test. The Mersenne numbers are defined by $M_k = 2^k - 1$. Recall that this can be prime only if k is a prime, and that the even perfect numbers are exactly those of the form $2^{\ell-1} M_\ell$ where M_ℓ is prime. We are thus interested in knowing when M_ℓ is prime.

The Lucas-Lehmer numbers are defined recursively by $s_1 = 4$ and $s_{n+1} = s_n^2 - 2$. The Lucas-Lehmer test says that, for ℓ a prime number, M_ℓ is prime if and only $s_{\ell-1} \equiv 0 \mod M_\ell$.

(1) Use the Lucas-Lehmer test to find all Mersenne primes M_ℓ with $\ell \leq 31$. Write down the corresponding perfect numbers.
(2) One direction of the Lucas-Lehmer test can be established using arithmetic in $\mathbb{Z}[\sqrt{3}]$ – read through this on p. 64 of Savin. We will discuss another proof using quadratic reciprocity after spring break.

Exercise 4. The sum of Euler's function on divisors. In this exercise we establish the following formula that is used in the proof of the existence of primitive roots (Proposition 20 on p.73 of Savin):

$$\sum_{d|n} \phi(d) = n.$$

(1) For $n = 15, 27$, and 100, verify this identity by computing the left-hand side.
(2) Here is one way to justify this identity in general:
   (a) For $n = p^k$, p prime, verify it holds by expanding the left-hand side (there will be a lot of cancellation in the sum!).
   (b) If it holds for $n = a, n = b$ with $\gcd(a, b) = 1$, verify it holds also for $n = ab$ (use the fact that $\phi(xy) = \phi(x)\phi(y)$ when $\gcd(x, y) = 1$).
   (c) Conclude.
(3) Here is a better way to justify it by a counting argument:
   (a) Let $d|n$, and write $d' = n/d$, so $dd' = n$. Show that there is a bijection between the integers $0 \le k \le d$ such that $\gcd(k, d) = 1$ and the integers $0 \le j \le n$ such that $\gcd(j, n) = d'$.
   (b) Conclude (if we apply (a) to each term in the sum, then what is the left-hand side counting?).

It turns out that any finite field has size a prime power, so that for the application to the existence of primitive roots in finite fields (e.g. for Diffie-Hellman), your argument in 2-(a) will suffice!

Exercise 5. Dirichlet's Theorem. Dirichlet's Theorem on primes in arithmetic progressions says that for any m and k with $\gcd(k, m) = 1$, there are infinitely many prime numbers p such that $p \equiv k \mod m$ (an equivalent statement is that the numbers $qm + k$ are prime for infinitely many values of q; a sequence of numbers of this form is called an arithmetic progression, thus the name of the theorem). The proof of this theorem, surprisingly, uses calculus to study convergence of certain series – you can see a sketch of the method in Savin - Chapter 4, Sections 1 and 2.

In certain special cases, however, this statement can be justified by an argument similar to Euclid's argument for the existence of infinitely many prime numbers:

(1) Show that there are infinitely many primes p such that $p \equiv 2 \mod 3$. (Hint: for $p_1, \ldots, p_n$ a collection of odd primes, consider the number $3p_1p_2 \ldots p_n + 2$).
(2) Can you prove any other cases? (See also Exercise 7-(2)).

Exercise 6. Cyclotomic polynomials.

(1) Read Savin - Chapter 5, Section 4 (starting on p.77), then complete the exercises for that section (starting on p.79).
(2) Give a Euclidean argument to show that for any m, there are infinitely many primes

$$p \equiv 1 \mod m.$$

(Hint: for $p_1, p_2, \ldots, p_n$ a set of primes, consider $\phi_m(p_1 \ldots p_n)$).