4400-001 - SPRING 2022 - WEEK 11 (3/29, 3/31)
FERMAT PRIMES AND MERSENNE PRIMES

Some of these exercises can be found in Savin - Chapter 7.

Exercise 1 (required). Variations on Pepin's test.
The nth Fermat number is $F_n := 2^{2^n} + 1$. Pepin's test says F_n is prime if and only if

$$3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n.$$

(1) Use Pepin's test to show that F_4 is prime.

(2) Let $n \geq 2$. Show that $F_n \equiv 2 \mod 5$.

(3) Let $n \geq 2$. Assume that F_n is prime. Use part (2) to show that $\left(\frac{5}{F_n}\right) = -1$.

(4) Following our justification for Pepin's test (see the Tuesday video), explain why for $n \geq 2$ the Fermat number F_n is prime if and only if $5^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$.

(5) Can a version of Pepin's test be developed with 7 instead of 3? How about with 11?

Exercise 2 (required). Some computations in $\mathbb{F}_p[i]$
Let p be a prime congruent to $3 \mod 4$, and let $\mathbb{F}_p[i]$ be the set of elements $a + bi$ where $a, b \in \mathbb{F}_p$ with $i^2 := -1$ – this is a field with p^2 elements (indeed, we can construct it also as $\mathbb{F}_p[x]/(x^2+1)$, where x is identified with i, which is a field since $x^2 + 1$ is a prime polynomial in $\mathbb{F}_p[x]$ in this case).

(1) Find a primitive root (i.e. a primitive $(p^2 - 1)$st root of unity) in $\mathbb{F}_3[i]$, and write down the corresponding discrete logarithm function $I : \mathbb{F}_3[i]^\times \to \mathbb{Z}/8\mathbb{Z}$.

(2) Show that any $d \in \mathbb{F}_p$ has a square root in $\mathbb{F}_p[i]$.

(3) Show that $(a + bi)^p = (a - bi)$. *Hint: for any x, y in a field containing $\mathbb{F}_p$, $(x + y)^p = x^p + y^p$.*

(4) The norm of an element $a + bi$ in $\mathbb{F}_p[i]$ is

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{F}_p$$

Show that for $x, y \in \mathbb{F}_p[i]$, $N(xy) = N(x)N(y)$.

(5) Deduce from (3) that $N(a + bi) = (a + bi)^{p+1}$

(6) Let $T(p)$ denote the elements $z \in \mathbb{F}_p[i]^\times$ such that $N(z) = 1$. Show that $T(p)$ is a *subgroup* of $\mathbb{F}_p[i]^\times$ – this means that if $x, y \in T(p)$ then $xy \in T(p)$ and $x^{-1} \in T(p)$.

(7) Deduce from (5) that there are exactly $p + 1$ elements in $T(p)$.

(8) For which $p \equiv 3 \mod 4$ is i a square in $\mathbb{F}_p[i]$?

(9) For which $p \equiv 3 \mod 4$ is i the square of an element in $T(p)$?

(10) If $p \equiv 1 \mod 4$, then we can still define $\mathbb{F}_p[i]$ as a ring, but it is not a field. Illustrate this in a specific case by finding a non-zero element in $\mathbb{F}_5[i]$ that is not invertible.
Hint: in any ring, a zero divisor *is an element x such that there is another non-zero element y with $xy = 0$. A zero divisor is never invertible – indeed, if x is is invertible then*

$$xy = 0 \implies x^{-1}xy = x^{-1}0 \implies y = 0.$$

Thus it suffices to find a non-zero zero divisor in $\mathbb{F}_5[i]$.

Exercise 3. Recall from Week 7 that the Mersenne numbers are defined by $M_k = 2^k - 1$; these can be prime only if k is a prime, and 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, and an algorithm is furnished by:

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

In Week 7 we spent some time in class using the Lucas-Lehmer test to find Mersenne primes (Week 7 - 3). This exercise builds on the video for Thursday to give a justification of the Lucas-Lehmer test.

Let $\alpha = 2 + \sqrt{3}$ and let $\beta = 2 - \sqrt{3}$.

(1) Show $\alpha\beta = 1$.

(2) Show $\alpha + \beta = s_1$.

(3) Assuming $\alpha^{2^{n-1}} + \beta^{2^{n-1}} = s_n$, show that $\alpha^{2^n} + \beta^{2^n} = s_{n+1}$.

Assuming (2) and (3), the principle of mathematical induction yields $s_n = \alpha^{2^{n-1}} + \beta^{2^{n-1}}$ for all $n \geq 1$. In the video for Thursday, we show:

Theorem. *M_ℓ is prime if and only if $\alpha^{2^{\ell-1}} \equiv -1 \mod M_\ell$.*

We now show this theorem is equivalent to the Lucas-Lehmer test:

(4) Show $s_{l-1} \equiv 0 \mod M_\ell$ if and only if $\alpha^{2^{\ell-2}} = -\beta^{2^{\ell-2}} \mod M_\ell$
(note that the latter is an identity mod M_ℓ in $\mathbb{Z}[\sqrt{3}]$).

(5) Show that $\alpha^{2^{\ell-2}} = -\beta^{2^{\ell-2}} \mod M_\ell$ if and only if $\alpha^{2^{\ell-1}} = -1 \mod M_\ell$
Hint: Multiply by $\alpha^{2^{\ell-2}}$ to go one way and by $\beta^{2^{\ell-2}}$ to go the other.

(6) Conclude.