Math 261 — Exam 2

November 4, 2017

The use of calculators, notes, and books is **NOT** allowed.

Exercise 1: Since today is November 4... (22 pts)

1. (8 pts) Factor 114 into irreducibles in $\mathbb{Z}[i]$.

   Make sure to justify that your factorization is complete.

2. (6 pts) Is 114 a sum of 2 squares ? Of 3 squares ? Of 4 squares ?

3. (8 pts) Given that $p = 1142017$ is prime, find the number of elements of $\mathbb{Z}[i]$ of norm p.

Solution 1:

1. First of all, $114 = 2 \times 3 \times 19$. Now, we know that $2 = -i(1+i)^2$, and since 3 and 19 are primes $\equiv -1 \pmod 4$, they are irreducible in $\mathbb{Z}[i]$. So the complete factorization is
$$114 = -i \times (1+i)^2 \times 3 \times 19.$$

2. Since there are primes (namely 3 and 19) that show up with odd multiplicity in 114, it is not a sum of 2 squares. However, 114 is not divisible by 4, so if it were of the form $4^a(8b+7)$ we would have $a = 0$ so $114 = 8b+7$, which is not the case, so 114 is a sum of 3 squares. A fortiori it is also a sum of 4 squares.

3. We see that $p \equiv 1 \pmod 4$, so p splits as $\pi\bar{\pi}$ in $\mathbb{Z}[i]$, with π and $\bar{\pi}$ non-associate irreducibles, both of norm p. So an element of $\mathbb{Z}[i]$ of norm p must factor as $u\pi$ or $u\bar{\pi}$, where u is a unit; since π and $\bar{\pi}$ are not associate, these elements are all distinct, and since there are 4 choices for u, we get 8 such elements.

Exercise 2: Legendre symbols (17 pts)

1. (5 pts) State the law of quadratic reciprocity.

2. (7 pts) Compute the Legendre symbol $\left(\dfrac{33}{79}\right)$.

   You may use without proof the fact that 79 is prime.

3. (5 pts) Solve the equation $x^2 = x + 8$ in $\mathbb{Z}/79\mathbb{Z}$.

Solution 2:

1. Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = (-1)^{p'q'} \left(\frac{q}{p}\right),$$

where $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$.

2.

$$\left(\frac{33}{79}\right) = \left(\frac{3}{79}\right)\left(\frac{11}{79}\right) = -\left(\frac{79}{3}\right) \times -\left(\frac{79}{11}\right) \text{ by quadratic reciprocity}$$

$$= \left(\frac{1}{3}\right)\left(\frac{2}{11}\right) = \left(\frac{2}{11}\right) = -1$$

since $11 \equiv 3 \pmod 8$.

3. The equation can be rewritten as $x^2 - x - 8 = 0$. Its discriminant is

$$\Delta = 1^2 - 4 \times -8 = 33,$$

and we have seen that $\left(\frac{33}{79}\right) = -1$, so the equation has no solutions in $\mathbb{Z}/79\mathbb{Z}$.

Exercise 3: A really big number (24 pts)

1. (6 pts) Prove that every integer $n \in \mathbb{N}$ is congruent to the sum of its digits mod 9.

2. (15 pts) Let $A = 4444^{4444}$, let B be the sum of the digits of A, let C be the sum of the digits of B, and finally let D be the sum of the digits of C. Compute D mod 9.

3. (3 pts) Deduce that $D = 7$.

Solution 3:

1. Let $n_0, n_1, n_2, \cdots$ be the digits of n from right to left, so that

$$n = n_0 + 10n_1 + 100n_2 + \cdots = \sum n_i 10^i.$$

Since $10 \equiv 1 \pmod 9$, we have

$$n = \sum n_i 10^i \equiv \sum n_i 1^i = \sum n_i \pmod 9.$$

2. By the previous question, we have $D \equiv C \equiv B \equiv A \pmod 9$, so we can just as well compute A mod 9.

   Now $4444 \equiv 16 \equiv -2 \pmod 9$, so $A \equiv (-2)^{4444} \pmod 9$. Now -2 and 9 are coprime, so by Fermat's little theorem we have $(-2)^{\phi(9)} \equiv 1 \pmod 9$. We have $\phi(9) = 6$, so we can replace the exponent 4444 by anything congruent to it mod 6. Since $4444 \equiv 4 \pmod 6$, we deduce that $A \equiv (-2)^4 = 16 \equiv 7 \pmod 9$.

3. We are going to estimate roughly the size of D. First of all, we have

$$A < 10000^{5000} = 10^{20000},$$

so A has at most 20000 digits, so

$$B \leqslant 9 \times 20000 = 180000.$$

So either B has 6 digits and the first one is a 1, or it has 5 digits or less; either way

$$C \leqslant 1 + 6 \times 9 = 55.$$

Therefore C has at most 2 digits and the first one is at most 5, so

$$D \leqslant 5 + 9 = 14.$$

Since we also know that $D \equiv 7 \pmod 9$, we conclude that in fact $D = 7$.

Exercise 4: A primality test (37 pts)

Let $p \in \mathbb{N}$ be a prime such that $p \equiv 3 \pmod 4$, and let $P = 2p+1$. The goal of this exercise is to prove that P is prime if and only if $2^p \equiv 1 \bmod P$.

1. In this question, we suppose that P is prime, and we prove that $2^p \equiv 1 \bmod P$.

   (a) (6 pts) Compute the Legendre symbol $\left(\frac{2}{P}\right)$.

   (b) (5 pts) Deduce that $2^p \equiv 1 \pmod P$.
   Hint: What is $\frac{P-1}{2}$*?*

2. In this question, we suppose that $2^p \equiv 1 \bmod P$, and we prove that P is prime.

   (a) (6 pts) Prove that $2 \in (\mathbb{Z}/P\mathbb{Z})^\times$. What is its multiplicative order?

   (b) (6 pts) Deduce that $p \mid \phi(P)$.

   (c) (9 pts) Prove that p and P are coprime, and deduce that there exists a prime divisor q of P such that $q \equiv 1 \pmod p$.
   Hint: $\phi(\prod p_i^{a_i}) = \prod (p_i - 1) p_i^{a_i - 1}$.

   (d) (5 pts) Deduce that P is prime.
   Hint: How large can P/q *be?*

Solution 4:

1. In this question, we suppose that P is prime, and we prove that $2^p \equiv 1 \bmod P$.

   (a) Since $p = 4k+3$, we have $P = 2p+1 = 8k+7 \equiv -1 \pmod 8$, so $\left(\frac{2}{P}\right) = 1$.

   (b) We have $2^p = 2^{\frac{P-1}{2}} \equiv \left(\frac{2}{P}\right) = 1 \pmod P$.

2. (a) Since $2^p \equiv 1 \pmod P$, we see that 2 is invertible mod P, of inverse 2^{p-1}. Also, the same formula tells us that its multiplicative order mod P is a divisor of p. SInce p it prime, it is thus either 1 or p. But if it were 1, we would have $2^1 \equiv 1 \pmod P$, which is impossible since $P = 2p+1 \geqslant 5$. So it must be p.

(b) Fermat's little theorem tells us that $p^{\phi(P)} \equiv 1 \pmod P$, so that $\phi(P)$ is a multiple of the multiplicative order of p mod P. But this order is p by the previous question.

(c) Since $P - 2p = 1$, p and P are coprime (Bézout). Let now $P = \prod p_i^{a_i}$ be the factorization of P. We have $\phi(P) = \prod (p_i - 1) p_i^{a_i - 1}$, and p divides this product by the previous question. Since p is prime, Euclid tells us that it must divide at least one of the factors. But p cannot divide any of the p_i since p and P are coprime, so p must divide at least one of the $(p_i - 1)$. Letting $q = p_i$, we have thus found a prime q such that $q \mid P$ and $q \equiv 1 \pmod p$.

(d) Since $q \equiv 1 \pmod p$ and $q \neq 1$, we have $q \geqslant p+1$, so $P/q \leqslant \frac{2p+1}{p+1} < 2$. But since $q \mid P$, P/q is an integer, so we must have $P/q = 1$. Therefore, $P = q$ is prime.

END