

## Practice problems for the Final Exam

Liubomir Chiriac

- (a) Let  $p \equiv 1 \pmod{4}$  be a prime. Prove that there exists some  $x \in \mathbb{Z}$  such that  $p \mid x^2 + 1$ .  
(b) Use the quadratic character of -1 to prove that there are infinitely many primes of the form  $4k + 1$ . (Hint: Assume that there are only finitely many such primes:  $p_1, \dots, p_r$ . Let  $q$  be a prime factor of  $N = 1 + 4(p_1 \dots p_r)^2$ . What is  $q \pmod{4}$ ?)
- Let  $a$  be a primitive root modulo an odd prime  $p$ .
  - Can  $a$  be a quadratic residue modulo  $p$ ? (Hint: Look at  $\text{ord}_p(a)$ .)
  - We have proved in class that the numbers  $a^1, a^2, \dots, a^{p-1}$  are congruent modulo  $p$ , in some order, to  $1, 2, \dots, p-1$ . Use this observation to show that

$$(p-1)! \equiv \left(\frac{a}{p}\right)^p \pmod{p}.$$

- Combining (a) and (b) give another proof of Wilson's Theorem.
- Let  $p$  be an odd prime. Use the Law of Quadratic Reciprocity to prove that

$$\left(\frac{3}{p}\right) = 1 \text{ if and only if } p \equiv 1 \pmod{12} \text{ or } p \equiv -1 \pmod{12}.$$

(Hint: Consider two separate cases depending on  $p \pmod{4}$ .)

- (a) Let  $a, b \in \mathbb{Z}$  such that  $a \neq 0$ . Prove that  $n = a^2 + b^2$  is not a Gaussian prime.  
(b) If  $x, y \in \mathbb{Z}[i]$  such that  $N(x) \mid N(y)$ , is it necessarily true that  $x \mid y$ ?
- Which elements of the set  $\{i + 1, 3 - 2i, 101i, 11 + 2i, -103i, 7 + 5i\}$  are Gaussian primes?
- Let  $p \geq 7$  be a prime. Prove that there exist two consecutive integers that are both quadratic residues modulo  $p$ . (Hint:  $2 \cdot 5 = 10$ .)

## SOLUTIONS

1. (a) Since  $p \equiv 1 \pmod{4}$ , it follows that  $-1$  is a quadratic residue modulo  $p$ . Thus,  $-1 \equiv x^2 \pmod{p}$  for some  $x \in \mathbb{Z}$ . This means that  $p \mid x^2 + 1$ .

(b) Assume that there are only finitely many primes  $p_1, \dots, p_r$  of the form  $4k + 1$ . Consider the number  $N = 1 + 4(p_1 \dots p_r)^2$ , and let  $q$  be a prime dividing  $N$ . Clearly,  $q \neq p_i$  for any  $i = 1, \dots, r$ . Also, since  $q \mid N$ , we get

$$-1 \equiv (2p_1 \dots p_r)^2 \pmod{q}.$$

Thus,  $-1$  is a quadratic residue modulo  $q$ , which happens precisely when  $q \equiv 1 \pmod{4}$ . This means that  $q$  is a prime of the form  $4k + 1$ , which is not in our initial list. This contradicts the finiteness assumption, so there are infinitely many primes of the form  $4k + 1$ .

2. (a) Assume that  $a$  is a primitive root modulo  $p$ , which is also a quadratic residue modulo  $p$ . On the one hand, by Euler's identity:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Since  $a$  is a quadratic residue, we obtain  $a^{(p-1)/2} \equiv 1 \pmod{p}$ , so  $\text{ord}_p(a) \leq (p-1)/2$ .

On the other hand  $a$  is also a primitive root, i.e.,  $\text{ord}_p(a) = p-1$ , which is a contradiction. Therefore, no primitive root  $a$  can be a quadratic residue modulo  $p$ .

(b) Just note that

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot \dots \cdot (p-1) \\ &\equiv a^{1+2+\dots+(p-1)} \pmod{p} \\ &\equiv a^{(p-1)p/2} \pmod{p} \\ &\equiv \left(\frac{a}{p}\right)^p \pmod{p}, \end{aligned}$$

where the last step follows from Euler's identity.

(c) From (a) we have that  $a$  is a quadratic nonresidue, so  $\left(\frac{a}{p}\right) = -1$ . Thus, (b) implies that

$$(p-1)! \equiv (-1)^p = -1 \pmod{p},$$

since  $p$  is odd.

3. We distinguish two cases depending on  $p \pmod{4}$ .

- If  $p \equiv 1 \pmod{4}$ , then by the Law of Quadratic Reciprocity followed by Euler's identity:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \equiv p^{(3-1)/2} \equiv p \pmod{3}.$$

Therefore  $\left(\frac{3}{p}\right) = 1$  if and only if  $p \equiv 1 \pmod{3}$ . Since  $p \equiv 1 \pmod{4}$  and  $p \equiv 1 \pmod{3}$ , it follows that  $p \equiv 1 \pmod{12}$ , in this case.

- If  $p \equiv -1 \pmod{4}$  a similar analysis shows that  $p \equiv -1 \pmod{12}$ .

4. (a) Note that we can factor  $n = (a + bi)(a - bi)$  in  $\mathbb{Z}[i]$ . If  $n$  is a Gaussian prime, then either  $a + bi$  or  $a - bi$  must be a unit. The only units in  $\mathbb{Z}[i]$  are  $\pm 1$  and  $\pm i$ . Since  $a \neq 0$ , it follows that  $a = \pm 1$  and  $b = 0$ . However, in that case  $n$  is a unit, so it cannot be a Gaussian prime (by definition).

(b). This is not necessarily true. One possible counterexample is given by  $x = 3 + 4i$  and  $y = 5$ . Clearly,  $N(x) = N(y) = 25$  so  $N(x) \mid N(y)$ . However,

$$\frac{5}{3 + 4i} = \frac{5(3 - 4i)}{(3 + 4i)(3 - 4i)} = \frac{5(3 - 4i)}{25} = \frac{3}{5} - \frac{4}{5}i,$$

which is not an element of  $\mathbb{Z}[i]$ . Thus,  $x \nmid y$ .

5. Recall that  $z \in \mathbb{Z}[i]$  is a Gaussian prime if and only if one of the following conditions holds:

- $N(z)$  is a prime integer,
- $z$  is a unit times a prime integer that is congruent to 3 (mod 4).

Now,  $1 + i$  and  $3 - 2i$  are Gaussian primes because their norms are prime integers. Also,  $-103i = (-i) \cdot 103$  is a Gaussian prime because  $(-i)$  is a unit and  $103 \equiv 3 \pmod{4}$ . The other three elements from the list are not Gaussian primes, because they do not meet any of above criteria. In fact, one can factor them into a product of two Gaussian integers, none of which is a unit:

$$\begin{aligned} 101i &= (10 + i)(1 + 10i), \\ 11 + 2i &= (1 + 2i)(3 - 4i), \\ 7 + 5i &= (1 - i)(1 + 6i). \end{aligned}$$

6. If  $p = 7$  the quadratic character of 2 gives that  $\left(\frac{2}{7}\right) = 1$ , so the pair (1, 2) works. Without loss of generality, assume  $p \geq 11$ . Consider the following three pairs of consecutive integers:

$$(1, 2), (4, 5) \text{ and } (9, 10).$$

It is clear that 1, 4 and 9 are all quadratic residues (since they are all squares). If either 2 or 5 is a quadratic residue modulo  $p$ , then one of the first two pairs satisfies the statement. Otherwise,

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{5}{p}\right) = (-1) \cdot (-1) = 1,$$

so the third pair works.