Practice problems for the Final Exam

Liubomir Chiriac

1. Let ℓ be an odd prime and let p be a prime factor of $2^\ell - 1$.
   (a) Prove that $\text{ord}_p(2) = \ell$.
   (b) Prove that $p \equiv 1 \pmod{\ell}$.
2. Consider the equation $\overline{x}^2 - \overline{3}\overline{x} + \overline{7} = \overline{0}$.
   (a) Find all solutions to this equation in $\mathbb{Z}_5$.
   (b) Find all solutions to this equation in $\mathbb{Z}_7$.
   (c) Find all solutions to this equation in $\mathbb{Z}_{35}$.
3. (a) Check that 2 is a primitive root modulo 19.
   (b) Find all primitive roots modulo 19.
4. Let $a, b \in \mathbb{Z}$ such that $a \neq 0$. Prove that $n = a^2 + b^2$ is not a Gaussian prime.
5. Let x and y be Gaussian integers.
   (a) Show that if $x \mid y$ then $N(x) \mid N(y)$.
   (b) If $N(x) \mid N(y)$, is it necessarily true that $x \mid y$? Prove it or find a counterexample.
6. Which elements of the set $\{1 + i, 3 - 2i, 101i, 11 + 2i, -103i, 7 + 5i\}$ are Gaussian primes?

Solutions

1. (a) Since p is a prime factor of $2^\ell - 1$ it follows that $2^\ell \equiv 1 \pmod{p}$. By Proposition 10.1.3 (i) we obtain that $\mathrm{ord}_p(2) \mid \ell$, so $\mathrm{ord}_p(2)$ is either 1 or ℓ. However, it is clear that $\mathrm{ord}_p(2) \neq 1$. Therefore, $\mathrm{ord}_p(2) = \ell$.

(b) Corollary 10.1.4 implies that $\mathrm{ord}_p(2) \mid p - 1$, which gives $p \equiv 1 \pmod{\ell}$ by part (a).

2. (a) Note that in $\mathbb{Z}_5$:

$$\overline{x}^2 - \overline{3}\overline{x} + \overline{7} = \overline{x}^2 - \overline{3}\overline{x} + \overline{2} = (\overline{x} - \overline{1})(\overline{x} - \overline{2}).$$

Thus the solutions are $\overline{x} = \overline{1}$ and $\overline{x} = \overline{2}$.

Alternatively, one could use the Quadratic Formula in $\mathbb{Z}_p$ (page 437), or just try directly all elements of $\mathbb{Z}_5$ and see which ones are actually solutions.

(b) Similarly, in $\mathbb{Z}_7$:

$$\overline{x}^2 - \overline{3}\overline{x} + \overline{7} = \overline{x}^2 - \overline{3}\overline{x} = \overline{x}(\overline{x} - \overline{3}),$$

which gives the solutions $\overline{x} = \overline{0}$ and $\overline{x} = \overline{3}$.

(c) Every solution in $\mathbb{Z}_{35}$ must be a solution simultaneously in $\mathbb{Z}_5$ and $\mathbb{Z}_7$. By part (a) we know that every solution satisfies either $x \equiv 1 \pmod{5}$ or $x \equiv 2 \pmod{5}$, and by part (b) we know that $x \equiv 0 \pmod{7}$ or $x \equiv 3 \pmod{7}$. Thus, there are four different possibilities to consider, and in each case we can use the Chinese Remainder Theorem to find the unique solution $\pmod{35}$.

- (Case 1): $x \equiv 1 \pmod{5}$ and $x \equiv 0 \pmod{7}$. Using the Chinese Remainder Theorem we find $x \equiv 21 \pmod{35}$.
- (Case 2): $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$. We find $x \equiv 31 \pmod{35}$.
- (Case 3): $x \equiv 2 \pmod{5}$ and $x \equiv 0 \pmod{7}$. We find $x \equiv 7 \pmod{35}$.
- (Case 4): $x \equiv 2 \pmod{5}$ and $x \equiv 3 \pmod{7}$. We find $x \equiv 17 \pmod{35}$.

In conclusion, the solution set in $\mathbb{Z}_{35}$ is $\{\overline{7}, \overline{17}, \overline{21}, \overline{31}\}$.

3. (a) We have to show that $\mathrm{ord}_{19}(2) = 18$. By Corollary 10.1.4 we know that $\mathrm{ord}_{19}(2)$ must be a divisor of 18, i.e., it is either 1,2,3,6,9 or 18. We rule out all the divisors less than 18 as follows:

Since $2^4 < 19$ we see that $\mathrm{ord}_{19} 2 > 4$. Moreover, $2^6 \equiv 7 \pmod{19}$ and $2^9 \equiv -1 \pmod{19}$.

Thus, the only possibility is that $\mathrm{ord}_{19}(2) = 18$, so 2 is a primitive root modulo 19.

(b) Theorem 10.3.7 says that there are $\varphi(18) = 6$ primitive roots modulo 19. As explained at the end of page 444 they are precisely

$$2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17} \pmod{19}.$$

It remains to reduce these powers of 2 modulo 19. This can be done, for example, using repeated squaring. One obtains that $2^5 \equiv 13 \pmod{19}$, $2^7 \equiv 14 \pmod{19}$, $2^{11} \equiv 15 \pmod{19}$, $2^{13} \equiv 3 \pmod{19}$, and $2^{17} \equiv 10 \pmod{19}$. Thus, the set of primitive roots modulo 19 is $\{2, 3, 10, 13, 14, 15\}$.

4. 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 an unit. The only units in $\mathbb{Z}[i]$ are ± 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).

5. (a) Since $x \mid y$, it follows that $y = x \cdot w$ for some $w \in \mathbb{Z}[i]$. Taking norms, we get

$$N(y) = N(x \cdot w) = N(x) \cdot N(w),$$

which shows that $N(x) \mid N(y)$.
(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, $x \nmid y$.

6. Recall (see Theorem on page 639) that $z \in \mathbb{Z}[i]$ is a Gaussian prime if and only if one of the following conditions holds:

(i) $N(z)$ is a prime integer,

(ii) 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 beacuse $(-i)$ is a unit and $103 \equiv 3 \pmod 4$. The other three elements from the list are not Gaussian primes, because they meet none of above criteria. In fact, one can factor them into a product of two Gaussian integers, none of which is a unit:

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