Math 4400/6400 – Review for the final exam
April 27, 2013

Learning objectives

Gaussian integers

- Give the basic definitions concerning the Gaussian integers, including the definition of the set $\mathbf{Z}[i]$, *conjugation*, the *norm* map, and *associates*.
- Demonstrate that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbf{Z}[i]$.
- Demonstrate the equivalence between two elements being associates and each being a unit multiple of the other.
- Describe the chain of reasoning that culminates in the proof of the unique factorization theorem.
- Formulate and prove the division algorithm for Gaussian integers.
- Explain the definition of the greatest common divisor in $\mathbf{Z}[i]$ and prove that every two Gaussian integers have a greatest common divisor. Be able to compute the greatest common divisor via Euclid's algorithm.
- Formulate the fundamental lemma, Euclid's lemma, and the theorem on unique factorization in $\mathbf{Z}[i]$. Give the main ideas of all of these proofs.
- Characterize the Gaussian primes π by determining how rational primes factor in $\mathbf{Z}[i]$. Relate this characterization back to the question of which primes can be written as sums of two squares.

Practice problems

1. If m and n are relatively prime, show that $\gcd(m+n, mn) = 1$.
2. How many incongruent solutions x are there to the congruence
$$15x \equiv 85 \pmod{2005}?$$
(*Incongruent* means distinct modulo 2005.) **Do not** find the solutions.

3. What are the last two digits of 107^{842}? *Hint:* Look mod 100 and use Euler's theorem.

4. Show that if a and b are positive integers and $a^3 \mid 2b^3$, then $a \mid b$.

5. Is there an integer solution (x, y) to the equation $15x^2 - 105y^3 = 7$?

6. Show that if p and $p+2$ are both prime numbers, then

$$4((p-1)!+1)+p \equiv 0 \pmod{p(p+2)}.$$

   Hint: Show that the left-hand side is divisible by both p and by $p+2$. Why is this enough? [You can also prove that the converse is true; whenever this congruence holds for an integer p, both p and $p+2$ have to be prime.]

7. The integer 2117 factors as $29 \cdot 73$.

   (a) Show that there are four incongruent solutions modulo 2117 to the equation $x^2 \equiv 1 \pmod{2117}$.

   (b) Say that the solutions solutions from (a) are x_1, x_2, x_3, x_4. Find the product $x_1x_2x_3x_4$ modulo 2117.

   Hint: Represent the solutions as elements of the ring $\mathbf{Z}_{29} \times \mathbf{Z}_{73}$.

8. Show that 3 is a primitive root modulo 17.

9. Let p be the prime 3331. Show that the list 1^3, 2^3, 3^3, $\ldots$, $(p-1)^3$ contain a repetition mod p. *Hint:* Notice that $p \equiv 1 \pmod 3$; use this to Show that in fact 1 is repeated.

10. Show that if p is an odd prime, then every primitive root modulo p is a quadratic nonresidue modulo p. Is the converse true?

11. Compute $\phi(450)$, $\tau(450)$, and $\sigma(450)$.

12. Let $\omega(n)$ represent the number of distinct primes dividing n. For example, $\omega(1) = 0$, and $\omega(6) = \omega(12) = 2$.

    (a) Show that $2^{\omega(n)}$ is a multiplicative function of n.

    (b) Explain why $\tau(n^2)$ is a multiplicative function of n. You may assume that τ is multiplicative.

(c) Show that for every natural number n,

$$\sum_{d|n} 2^{\omega(d)} = \tau(n^2).$$

13. Find all positive integers n for which $\sigma(n) = n + 6$. *Hint:* $\sigma(n) - n$ represents the sum of all of the divisors of n that are less than n.

14. Let p be an odd prime.

    (a) Prove that there are $\frac{p-1}{2}$ quadratic residues modulo p and $\left(\frac{p-1}{2}\right)$ quadratic nonresidues modulo p. [This proof should be in your notes.]

    (b) Show that

    $$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

    (c) Explain why, if $p \equiv 1 \pmod 4$, we in fact have

    $$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = 0.$$

15. Is there a solution x to the congruence $x^2 \equiv -10 \pmod{719}$? Note that 719 is a prime number.

16. Is there an integer x for which $x^4 \equiv -1 \pmod{2013}$? Justify your answer. Note that $2013 = 3 \cdot 11 \cdot 61$.

17. Let $\alpha = a + bi \in \mathbf{Z}[i]$. Show that if $1 + i \mid a + bi$ exactly when a and b have the same parity (i.e., are both even or both odd).

18. Suppose that π is a Gaussian integer of norm 49.

    (a) Show that $\pi \mid 7$. *Hint:* Recall from class we already showed that π divides some rational prime p.

    (b) Show that π is one of $7, -7, 7i$ or $-7i$.

19. Find a greatest common divisor of $4 + 6i$ and $4 - 6i$. (You do not have to use the Euclidean algorithm to solve this problem, but you may if you like!)

20. Find all Gaussian integers of norm 289. Justify your answer.