

## Session 14, July 26

### Prime Gaussian Integers, Encryption

1. What makes a number prime?
2. Why is the number 1 *not* prime in  $\mathbf{Z}$ ?
3. Why is the number 13 prime in  $\mathbf{Z}$ ? Why is the number 10 *not* prime in  $\mathbf{Z}$ ?
4. Which of these members of  $\mathbf{Z}[i]$  are prime:  $1, i, (1+i), (2+i), (3+i), (6+5i), (7+5i), (21+i)$ ? For each, explain how you know.
5. We noted previously that  $(3+2i)(5-3i) = (21+i)$ . This shows that  $(21+i)$  is not prime. Compute the norm of each piece of this product.

As previously noticed, if  $x$  and  $y$  are elements of  $\mathbf{Z}[i]$ , then  $N(xy) = N(x)N(y)$ .

6. Suppose an element of  $\mathbf{Z}[i]$  has a norm which is a prime in  $\mathbf{Z}$ . Explain why this means that the element must be prime in  $\mathbf{Z}[i]$ .
7. Why is the number 13 *not* prime in  $\mathbf{Z}[i]$ , even though it is prime in  $\mathbf{Z}$ ?
8. Which primes in  $\mathbf{Z}$  are also prime in  $\mathbf{Z}[i]$ ?

In the integers, the “Sieve of Eratosthenes” is a common method for finding prime numbers. The Sieve begins by listing the positive integers. 1 is eliminated, since it is not prime. Then, the smallest remaining number (2) is circled as a prime. To continue, all the multiples of the circled number are eliminated as non-primes (multiples of the prime), and the smallest remaining number is circled.

In other words, circle 2, dump its multiples. Circle 3, dump its multiples. Circle 5 (since 4 was dumped), and so on. Note that if we used the Sieve on all of  $\mathbf{Z}$ , we would circle 2 *and*  $-2$  as prime, then 3 *and*  $-3$ , etc.

9. Using a piece of graph paper, adapt the Sieve method to work to find primes in  $\mathbf{Z}[i]$ . What is (are) the “smallest” primes? How would you eliminate the multiples of a prime? How would you identify the “smallest” remaining prime to continue the Sieve? Continue as long as you like (a good stopping point is at norm = 50, but go as far or near as you feel comfortable).

Unique prime factorization is valid in  $\mathbf{Z}[i]$ , once you allow any primes which are equivalent up to units to be the same number. The proof is very similar to the one in  $\mathbf{Z}$ , and relies on the multiplicity of norms.

Some research in prime number theory involves primes in systems like  $\mathbf{Z}[i]$  and polynomials. Finding an underlying structure to the primes in  $\mathbf{Z}[i]$ , potentially geometrically, could explain the structure of primes in  $\mathbf{Z}$ , but no one has yet determined a complete structure to the primes.

Our last major topic is encryption methods.

10. Cryptanalyze this: K WOCCKQO VSUO DRSC YXO NYOCX'D BOWKSX  
COMBOD PYB VYXQ.
11. The encryption method used in Problem 10 is sometimes called a *shift cipher*. Do you see why?

It isn't hard to explain the shift cipher mathematically, once we agree on some labeling for the letters. Throughout, we are going to use  $A = 0, B = 1, C = 2, D = 3, \dots, Z = 25$ . In equations, we'll use the letter  $\mathbf{C}$  to represent "ciphertext", or encrypted text, and  $\mathbf{P}$  to represent "plaintext", or decrypted text. So, the basic issue in encryption is to make it very difficult for someone intercepting ciphertext to decrypt it, while making decryption easy for someone who knows how. In other words, there is an *encrypting algorithm* and a *decrypting algorithm*, and the decrypting algorithm undoes the encrypting algorithm.

12. If  $\mathbf{C}$  is a ciphertext letter and  $\mathbf{P}$  is a corresponding plaintext letter, write an equation that describes the decrypting algorithm for the (not very securely) encoded text in Problem 10.
13. If  $\mathbf{P}$  is a plaintext letter and  $\mathbf{C}$  is a ciphertext letter, write the encrypting algorithm for Problem 10.

Much of the work in encrypting and decrypting is done in mod's, and mod 26 is the most common starting point. There are 26 possible shift ciphers in mod 26 (including a shift of zero!). Most news and mail reading programs have available ROT13 encryption, a way to hide text which would either be a spoiler or off-color. "ROT13" stands for ROTate 13 letters.

Another type of encrypting algorithm is called a *multiplication cipher*. The following is a message encoded with a multiplication cipher in mod 26.

14. Cryptanalyze this: FVYC QNM YCN'F KIGV VAZJMZ FVAN NIKDMZ FMN.
15. Write an equation that describes the decrypting algorithm for the encoded text in Problem 14.
16. Write an equation that describes the encrypting algorithm for Problem 14.
17. Is  $\mathbf{C} = 2\mathbf{P} \pmod{26}$  a good encryption? Explain why. Are there 26 possible multiplication ciphers? If not, how many?
18. How many possible multiplication ciphers are there in mod 27? in mod 28? in mod 29?
19. Describe the steps you would take to solve the equation  $Ax + B = C \pmod{26}$ , and explain why and under what conditions (on  $A, B,$  and  $C$ ) the steps would not be possible.
20. Repeat Problem 19 for mod 29.

Linear, or *affine*, ciphers are of the form  $\mathbf{C} = m\mathbf{P} + b \pmod{n}$ . The modulus,  $n$ , must be at least as high as the number of letters used in the message;  $n = 26$  is frequent, but so is  $n = 29$ , which gives greater freedom for choices of the multiplier,  $m$ .  $n = 676$  allows for double-letter encryption, in which each pair of letters is written as a number (a two-digit number in base 26, actually!). In any case, decrypting a multiplication cipher boils down to finding the *inverse* of a number in a mod, something which we might be pretty good at by now...

21. DVAYA YMZML LAZGW AJVGT CEIQE DAD (in mod 26, spaced removed and adjusted).
22. Find  $k$  so that  $\mathbf{P} = k\mathbf{C} \pmod{676}$  is the decrypting algorithm for  $\mathbf{C} = 23\mathbf{P} \pmod{676}$ . In other words, find  $k$  in mod 676 so that  $23k = 1$ .

Tomorrow we will look at power ciphers and the public-key encryption system. Here are some related questions.

23. What is the value of  $32^{60}$  in mod 61? How do you know (quickly) what the answer is?
24. What is the value of  $32^{61}$  in mod 61? (Use the answer from Problem 23!)
25. What is the value of  $23^{48}$  in mod 65? How do you know? What makes composite numbers different than primes here?
26. What is the value of  $23^{49}$  in mod 65?