

MATH 100 - MORE NOTES AND SOLUTIONS TO WORKSHEETS 4, 4B

We are considering three types of problems:

- Solve $ax = b$
- Solve $ax = 1$ (invertibility)
- Solve $xy = b$ (factor)

in three types of systems:

- integers mod n , \mathbb{Z}_n
- integers \mathbb{Z}
- Gaussian integers $\mathbb{Z}[i]$.

The questions are:

- Can they be solved?
- If so, how?
- If so, how many solutions?

Historically, the motivation was just scientific curiosity, but we will see applications, in particular to cryptography.

Here is a summary of the principles we use.

The equation $ax = b \pmod n$ has a solution if and only if every divisor of both a and n is also a factor of b . We saw this both from observing the multiplication tables of \mathbb{Z}_n , and from looking at the equation $ax = b + qn$. When there is a solution, then there are d of them, where d is the greatest common divisor of a and n . Moreover, we have an efficient method for finding the solutions when the numbers are not too large.

When $a \not\equiv 0 \pmod n$ and n is prime, there is always a solution to $ax = b \pmod n$.

The element a is *invertible* if $ax = 1$ has a solution. Note that 0 is never invertible, while ± 1 always are. If p is prime, then every nonzero element in \mathbb{Z}_p is invertible.

Every element in the integers or Gaussian integers has a unique factorization into primes. The primes in \mathbb{Z} you know. The Gaussian primes are ordinary primes p that are congruent to $3 \pmod 4$, $1 \pm i$, and $a + bi$ where $a^2 + b^2$ is a prime that is congruent to $1 \pmod 4$.

No prime number that is $3 \pmod 4$ can be written as a sum of two squares. No number that has such a prime factor occurring an odd number of times in its prime factorization is a sum of two squares. Everything else is a sum of two squares. These statements seem complicated, but they are not so bad once you get used to them.

1. WORKSHEET 4 SOLUTIONS

- (1) What are the invertible elements in
- (a) \mathbb{Z} ? $1, -1$
 - (b) $\mathbb{Z}[i]$? $1, -1, i, -i$
 - (c) \mathbb{Z}_7 ? $1, 2, 3, 4, 5, 6$
 - (d) \mathbb{Z}_{12} ? $1, 5, 7, 11$
 - (e) \mathbb{Z}_{20} ? $1, 3, 7, 9, 11, 13, 17, 19$

Date: February 11, 2008.

- (f) \mathbb{Z}_{101} ? $1, 2, 3, \dots, 100$ because 101 is prime.
- (2) Factor these numbers into primes in \mathbb{Z} .
- (a) $68 = 2^2 \cdot 17$
 - (b) 113 is prime
 - (c) $600 = 2^3 \cdot 3 \cdot 5^2$
 - (d) $1414 = 2 \cdot 7 \cdot 101$
- (3) Write as the sum of two squares if possible.
- (a) $13 = 3^2 + 2^2$
 - (b) 15 not possible
 - (c) $17 = 4^2 + 1^2$
 - (d) 19 not possible
 - (e) $29 = 5^2 + 2^2$
 - (f) 203 not possible
 - (g) 77 not possible
 - (h) $85 = 9^2 + 2^2 = 7^2 + 6^2$
- (4) Factor these numbers into primes in $\mathbb{Z}[i]$.
- (a) 11 is prime
 - (b) $13 = (3 + 2i)(3 - 2i)$
 - (c) $15 = 3(2 + i)(2 - i)$
 - (d) $17 = (4 + i)(4 - i)$
 - (e) $63 = 3^2 \cdot 7$
 - (f) $73 = (8 + 3i)(8 - 3i)$

2. WORKSHEET 4B SOLUTIONS

- (1) What are the invertible elements in
- (a) \mathbb{Z}_{15} ? $1, 2, 4, 7, 8, 11, 13, 14$
 - (b) \mathbb{Z}_{21} ? $1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$
 - (c) \mathbb{Z}_{79} ? $1, 2, \dots, 78$
- (2) Factor these numbers into primes in \mathbb{Z} .
- (a) 73 is prime
 - (b) $117 = 3^2 \cdot 13$
 - (c) $238 = 2 \cdot 7 \cdot 17$
 - (d) $243 = 3^5$
- (3) Write as the sum of two squares if possible.
- (a) $53 = 7^2 + 2^2$
 - (b) 57 not possible
 - (c) 123 not possible
 - (d) 129 not possible
 - (e) $130 = 11^2 + 3^2 = 9^2 + 7^2$
- (4) Factor these numbers into primes in $\mathbb{Z}[i]$.
- (a) $37 = (6 + i)(6 - i)$
 - (b) $39 = 3(3 + 2i)(3 - 2i)$
 - (c) $41 = (5 + 4i)(5 - 4i)$
 - (d) 43 is prime
 - (e) $2 + i$ is prime
 - (f) $3 + i = (1 + i)(2 - i)$
 - (g) $3 + 2i$ is prime
 - (h) $3 + 4i = (2 + i)^2$