

Session 5, July 13

Linear Diophantine Equations

1. Find all elements of \mathbf{U}_7 , of \mathbf{U}_{15} .
2. How many elements are in \mathbf{U}_{29} ? In \mathbf{U}_{47} ? In \mathbf{U}_{997} ? Any conjectures?
3. (Geometry?!) Does the line $5x + 8y = 1$ pass through any lattice points? How about $6x + 3y = 1$?

Note: Lattice points are coordinates (x, y) where x and y are integers.

In today's session, we will look at equations of the form $ax + by = c$. These Linear Diophantine equations are closely related to greatest common divisors and Euclid's algorithm.

4. Find an integral solution (x, y) – if any exists – to each of the following equations. If no solution exists, find the smallest positive integer c for which $ax + by = c$ has a solution. Any conjectures?
 - (a) $5x + 8y = 1$
 - (b) $3x + 18y = 1$
 - (c) $7x + 13y = 1$
 - (d) $24x + 30y = 1$
 - (e) $11x + 9y = 1$

Euclid's algorithm is not just a nice method for calculating GCDs; analyzing it leads to some central theorems in number theory. For example, let's pick apart the calculation of the GCD of 216 and 3162.

$$\begin{array}{rcl}
 3162 & = & 14 \cdot 216 + 138 \\
 216 & = & 1 \cdot 138 + 78 \\
 138 & = & 1 \cdot 78 + 60 \\
 78 & = & 1 \cdot 60 + 18 \\
 60 & = & 3 \cdot 18 + 6 \\
 18 & = & 3 \cdot 6 + 0
 \end{array}$$

So, $\gcd(216, 3162) = 6$. Now, solve for the remainder in each of the divisions.

$$\begin{array}{rcl}
 138 & = & 3162 - 14 \cdot 216 \\
 78 & = & 216 - 1 \cdot 138 \\
 60 & = & 138 - 1 \cdot 78 \\
 18 & = & 78 - 1 \cdot 60 \\
 6 & = & 60 - 3 \cdot 18
 \end{array}$$

Then, start with the last equation, and inductively back-substitute, simplifying at each step.

$$\begin{aligned}
 6 &= -3 \cdot 18 + 60 \\
 &= -3(78 - 1 \cdot 60) + 60 = 4 \cdot 60 - 3 \cdot 78 \\
 &= 4(138 - 1 \cdot 78) - 3 \cdot 78 = -7 \cdot 78 + 4 \cdot 138 \\
 &= -7(216 - 1 \cdot 138) + 4 \cdot 138 = 11 \cdot 138 - 7 \cdot 216 \\
 &= 11(3162 - 14 \cdot 216) - 7 \cdot 216 = -161 \cdot 216 + 11 \cdot 3162
 \end{aligned}$$

We find that $6 = -161 \cdot 216 + 11 \cdot 3162$. Thus, 6 can be written as a linear combination of 216 and 3162.

5. Using any method, write the GCD of each pair of integers as a linear combination of the integers. (Suggestion: Do as many as it takes until you feel comfortable with the back-substitution process.)

(a) 12 and 16 (b) 3 and 14 (c) 128 and 1028

(d) 47 and 25 (e) 12 and 28 (f) 3 and 16

(g) 3 and 19 (h) 124 and 1024 (i) 36 and 124

6. Write 50 as a linear combination of 3 and 6.
7. Which integers can be written as a linear combination of 4 and 14?
8. Show that the numbers that can be written as linear combinations of 124 and 1028 are precisely the multiples of 4.
9. Use Euclid's algorithm and specific examples to explain why the following theorem holds:
If a and b are integers, there exist integers x and y so that $ax + by = \gcd(a, b)$.
10. Consider the linear Diophantine equation $47x + 25y = 2000$.
- (a) Find an integral solution (x, y) to this equation.
 (b) Find all positive integral solutions (x, y) to this equation.
11. Given two integers a and b , when can *every* integer be written as a linear combination of a and b ? Explain your reasoning.

Back to more modular arithmetic...

12. Which integers are equal to 2 in \mathbf{Z}_{10} ? Which integers are equal to 1 in \mathbf{Z}_{15} ?
13. Find the multiplicative inverse of 3 in \mathbf{Z}_{14} .
14. Find the multiplicative inverse of 4 in \mathbf{Z}_{15} .
15. Suppose p is prime. Explain why every non-zero element in \mathbf{Z}_p is a unit.
16. Suppose a and n are relatively prime. Show that a is a unit in \mathbf{Z}_n .

17. Consider $\mathbf{U}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$.
- (a) What is the inverse of 2? What is the inverse of 7? What is the inverse of $2 \cdot 7$? Any conjectures?
 - (b) What is the inverse of 8? What is the inverse of -8 ?
 - (c) In ordinary arithmetic, $a \cdot b = (-a) \cdot (-b)$. Does this work in \mathbf{U}_{15} ? Explain.
18. (Further exploration #1) The Post Office has only 5 and 8 cent stamps today. Which denominations of postage can you buy?
19. (Further exploration #2) Imagine a game played with pebbles. Player A has n pebbles and player B has m pebbles. Suppose $m < n$. Then B takes m pebbles away from A, putting them in a bowl that is “out of play.” Then the person with the fewest pebbles (which could be B again) takes her number away from the other person, putting them in a bowl. This continues until one person is out of pebbles. The other person wins. How many pebbles (in terms of m and n) are left in the winner’s pile?
- (Try playing this game with someone. Maybe let $m = 11$ and $n = 29$?)
20. (Further exploration #3) Show that \mathbf{Z}_{10} is a group under addition. Show that \mathbf{U}_{10} is a group under multiplication.