Session 4, July 12
Euclid's Algorithm

Reminder: The Division Algorithm

Given two integers a and b ($b \neq 0$), there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

1. Build addition and multiplication tables for $\mathbf{Z}_{12}$. Which numbers have opposites? Which numbers have inverses?
2. Without building an addition table, which numbers in $\mathbf{Z}_{24}$ have opposites?
3. Without building a multiplication table, which numbers in $\mathbf{Z}_{24}$ have inverses?
4. Solve each of the following in $\mathbf{Z}_{12}$:
   (a) $5x + 4 = 3$
   (b) $4x + 4 = 0$
   (c) $3x + 4 = 5$
5. Repeat Problem 4 in $\mathbf{Z}_7$. How is $\mathbf{Z}_7$ different from $\mathbf{Z}_{12}$?

In this session and in the sessions that follow, we will be exploring Euclid's algorithm, an application of the division algorithm.

6. Perform Euclid's algorithm on each pair of numbers below. What does the solution of this algorithm represent?
   (a) (11, 29) (b) (188, 1024) (c) (189, 1024)
   (d) (1717, 505) (e) (940, 5120) (f) (216, 3162)
7. Find the greatest common divisor (GCD) of 940 and 5120.
8. Find all common divisors of 940 and 5120. How are they related to gcd(940, 5120)?
9. Repeat Problems 7 and 8 using 312 and 1224.
10. Write a precise mathematical definition of the greatest common divisor of two integers a and b. The following definition will help:

    Let a and d be integers. We say that $d \mid a$ ("d divides a") if there is an integer k such that $a = dk$. (So... $7 \mid 280$ is a true statement, but $7 \mid 281$ is a false statement.)
11. Prove or Disprove or Salvage if Possible (Convincing arguments with numerical examples are OK.)
    (a) $a \mid a$
    (b) If $a \mid b$ and $b \mid c$, then $a \mid c$.
    (c) If $a \mid b$, then $b \mid a$.
    (d) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

12. Use your work in Problem 6(a) to show that

$$\frac{29}{11} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

This is the *simple continued fraction* for $\frac{29}{11}$.

13. These are the *convergents* of the simple continued fraction in Problem 12.

$$2, \qquad 2 + \frac{1}{1}\,, \qquad 2 + \cfrac{1}{1 + \cfrac{1}{1}}\,, \qquad 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}$$

Plot the values of all the convergents on a number line and observe carefully relations between the convergents and the fraction itself as well as the relations of the convergents to one another. What is going on?

14. Find the GCD of each pair of integers. Use any method you'd like. Any conjectures?

(a) (12, 16) (b) (12, 28)

(c) (6, 28) (d) (6, 34)

(e) (12, 17) (f) (17, 12) (g) $(17 + 25 \cdot 12, 16)$ (h) $(17 + 12k, 16), k \in \mathbf{Z}$

(i) (216, 3162) (j) (138, 216) (k) (78, 138) (l) (60, 78)

15. Explain why Euclid's algorithm correctly gives the greatest common divisor of two integers.

16. (Further Exploration) Expand $\sqrt{3}$ into a simple continued fraction. Do the same for $\sqrt{7}$. How accurate are these fractions after calculating, say, the fifth convergent?

Some left over fun problems from Session 3...

17. The quadratic equation $x^2 - x = 0$ has four solutions, or roots, in $\mathbf{Z}_{10}$. What are they? Why is this happening?! Why can't this happen in ordinary arithmetic?

18. Find all solutions to $x^2 - 6x + 8 = 0$ in $\mathbf{Z}_5$, in $\mathbf{Z}_{15}$, in $\mathbf{Z}_{105}$. Do the solutions you get in $\mathbf{Z}_5$ help you find solutions in $\mathbf{Z}_{15}$?

19. Suppose a number is written as a repeating decimal in base ten. Must it be a repeating decimal in every other base? If yes, explain why. If no, are there any particular bases in which it *must* be a repeating decimal?

Ways to Think about it

Euclid's algorithm can be illustrated with area, too. Suppose, for example, we want gcd(24, 30). Draw a 24×30 rectangle and fill it with squares. Start with the largest square that has a side of the rectangle as its side. That is the 24×24 square. Exactly one of these can be formed. This leaves a 24×6 rectangle on the right. The largest square possible is now 6×6. Exactly four of these can be formed. The original rectangle is filled. Since 6 is itself a divisor of 24, the 6×6 square could be used to tile the 24×24 square and indeed, the entire rectangle. Thus 6 is the greatest common divisor of 24 and 30. This can be illustrated as follows: