Solving discrete problems — Math 2020, Spring 2005

Schedule
For Thursday, January 20, 2005.

1. Sort out grading contract.
2. Review basic arithmetic.
3. Quick exercise: How many factors does 123456 have?
4. Introduction to proof by contradiction.

Break

5. Proof of unique factorisation.
6. Algorithm for finding factorisation — why do you only need to check upto the square root?
7. **What if not...** an example of a world where unique factorisation does not hold.

Basic arithmetic
(make sure you know all these)

1. Notation: The letter **Z** (from the German "Zahlen", meaning "number") is used to denote the set of integers.
2. Multiple: If a and b are positive integers, a is a multiple of b if there is some integer c so that $a = b \times c$.
3. Divisor: If a and b are positive integers, a is a divisor of b if there is some integer c so that $b = a \times c$.
4. If a and b are positive integers, When we say that a goes into b q times with remainder r, we mean that q and r are integers such that $b = aq + r$, and $0 \leq r < a$.
5. A prime is a positive integer with no divisors except itself and 1.
6. Positive integers a and b are relatively prime if the only number dividing both of them is 1.
7. The prime factorisation of an integer a is an expression of the form $a = p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_m^{n_m}$.
This is unique up to order of the factors. (You will be expected to be able to prove this result; we'll do this in class.)
8. The least common multiple of two integers a and b is the smallest integer n which is divisible by both a and b.
9. The greatest common divisor of two integers a and b is the largest integer which divides both of them.

Homework
(hand in on Tuesday 25 January)

1. Find the prime factorisations of each of the following numbers, and calculate the number of divisors of each.

$$54,\ 484,\ 900,\ 210^{10},\ 6^{(6^6)},\ 1940400,\ 637995160.$$

2. For any positive integer n, the factorial, n-factorial, is written $n!$ and is defined by

$$n! = 1 \times 2 \times 3 \times \cdots \times (n-1) \times n.$$

Verify the following:

$$\begin{aligned} 4! &= 5^2 - 1^2 = 7^2 - 5^2 \\ 5! &= 11^2 - 1^2 = 13^2 - 7^2 \\ 6! &= 27^2 - 3^2 = 28^2 - 8^2 = 29^2 - 11^2 \end{aligned}$$

When can $n!$ be written as the difference of two squares, and more generally, in how many ways can this be done? What happens for 7! and 11!?

3. Find the smallest integer, one half of which is square, one third of which is a cube, and one fifth of which is a fifth power. Write your answer as a product of primes.
4. Prove that the product of two numbers of the form $3n + 1$ also has this form.
5. Let $\mathcal{A} = \{2, 4, 6, 8, \cdots\}$ be the set of all even numbers. We'll say a number in $\mathcal{A}$ is prime if it can't be written as a product of two numbers in $\mathcal{A}$, both of which are smaller. Do we have unique factorisation in $\mathcal{A}$?

(Acknowledgement: These questions were taken from a course given by Peter Taylor at Queen's university, Canada)

Preparation
for class on Tuesday 25 January. This preparation is a review of algebra.

Factoring in algebra, of polynomials with integer coefficients, is similar to factoring in the integers —
We restrict to polynomials in one variable, with coefficients in the integers, and leading coefficient positive.
I.e., polynomials of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n$ are integers, and $a_n > 0$. The **degree** of this polynomial is n.
A **prime polynomial** is one that can't be written as a product of polynomials of smaller degree.

Exercise: Find the factorisations of the following polynomials into "prime" polynomials with integer coefficients:

1. $a^2 - 25$	3. $a^3 - 7^3$	5. $x^4 - 81$	7. $x^8 - 1$
2. $x^2 - 9$	4. $x^6 - 8$	6. $x^5 - 32$	8. $2a^3 + a - 3$

Useful fact to know: If $f(x)$ is a polynomial and $f(b) = 0$, then $(x - b)$ is a factor of $f(x)$. (Can you prove this?)
Example: if $f(x) = 2x^5 + 2x - 4$, then $f(1) = 0$, so $(x - 1)$ is a factor of $2x^5 + 2x - 4$.
In fact, $2x^5 + 2x - 4 = (x - 1)(x^4 + x^3 + x^2 + x + 2)$.