Howard University Math Department

Some problems from basic number theory

For the definition and explanation of strong induction, read Raji's book (Section 1.2.3, page 12) and the Discrete Math book (Section 2.5, Page 108). Raji's book has a simpler explanation.

Basically you use strong induction when you need to use not just the previous (n-th) step but other steps before that, in order to prove the n+1-th step.

1. Prove that any positive integer different from 1 can be factored into prime numbers in only one way. (Unique factorization of integers).

   Solution:

   If an integer is not a prime, then you can break it into factors (which *have* to be smaller than itself and bigger than 1). Then you can repeat the argument for its factors in case any of them is not a prime number. This process can be continued until you reach a factorization into prime numbers.

   In order to make this a rigorous argument, we need to use strong induction.

   The basis step is to show that 2 is a product of primes. But this is easy since 2 itself is a prime. Note that 1 is not a prime number and so it cannot be factored into a product of primes.

   Now assume that every positive integer different from 1 and smaller than a given positive integer n can be factored into a product of primes.

   If n itself is a prime, then we are done.

   If it is not a prime, it can be factored into $n = mk$ where $1 < m < n$, $1 < k < n$.

   But then the induction hypothesis applies to both m and k because both are smaller than n and different from 1.

   So they can both be factored into a product of primes and thus n itself can be factored into a product of primes.

   You can also show that this can be done in only one way. We will prove that below.

2. Prove that gcd of a and b (denoted (a, b)) is least positive element in set of integers of the form of $ax + by$ where x, y are integers.

   [Note that we are assuming such a number exists. But this follows from the well-ordering principle – any non-empty subset of natural numbers will contain a gcd].

   Solution: Suppose d_0 is the smallest natural number of the form $ma + nb$, and say $d_0 = m_0a + n_0b$. Let d be any natural number that divides both a and b. We will first

show that d also divides d_0. This means that the d_0 is bigger than any common divisor of a and b.

Proof that d divides d_0 : By the homework problem, if d divides a and b then d divides any number of form $ma + nb$. Therefore $d|d_0$ because it is of that form.

Next we will show that d_0 would also divide a and b which means it is also itself a common divisor of a and b. But since we already showed that it is bigger than any other common divisor, this means that d_0 IS the gcd of a and b.

To show this use division algorithm again, dividing a by d_0.

$$a = qd_0 + r,\ 0 \leq r < d \implies a = q(m_0a + n_0b) + r \implies (1 - qm_0)a + (-n_0)b = r.$$

So we get that $0 \leq r < d$ and r is of the form $ma + nb$.

Since d_0 is least such number only possibility is $r = 0$ and $d_0|a$.

Proof that $d_0|b$ is identical.

3. Prove by contradiction: If $p|ab$, then $p|a$ or $p|b$. (This is used to prove unique factorization).

   Solution: Let $ab = pk$ since p divides ab. Since p is prime, gcd of p and a is 1 if p does not divide a. So using problem 4, we can write $px + ay = 1$ for some integers x, y. Multiplying both sides by b we get $pbx + aby = b \implies pbx + (pk)y = b \implies p(bx + ky) = b$. In other words, p divides b. So if p doesn't divide a it will divide b. Same kind of argument can be used to show that if p doesn't divide b it will divide a.

   (Assuming unique factorization): Break down both a and b into prime factors. If p is not any one of them, then writing $a \times b$ as a product of primes we get a factorization of ab into primes that does not contain p. But we know there is only one way to do it, so it must be *the way* to factorize ab and thus p is not in the factorization of ab. In other words, p does not divide ab, contrary to assumption.

4. Prove that a positive integer n different from 1 can be factored into primes in only one way.

   Solution:

   Proof is by contradiction.

   Suppose if there are two ways to write n as a product of primes.

   $$n = p_1p_2....p_k = q_1q_2....q_m.$$

   Note that some of the primes p_i and q_i may be the same. Now any of the p_i that are the same as any of the q_i can be canceled out. So now let the following be the factorization of n after cancellation.

   $$n = p_{i_1}p_{i_2}....p_{i_k} = q_{j_1}q_{j_2}....q_{j_m}.$$

Now none of the p's are the same as any of the q's.

But from problem 3 we know that if a prime p divides a product it divides one of the factors of that product. So by writing the RHS as a product we can eventually show (this can be done by induction as well, see Lemma 5 of section 2.3.1 in Raji's book) that p_{i_1} is the same as one of the q's. This contradiction shows that all of the p's and q's will cancel out in the first place. So each of the p's equals one of the q's and they are all the same except for the order in which they are written.

5. (From Discrete math book) Use mathematical induction to show that postage of four cents or more can be achieved by using only 2-cent and 5-cent stamps.

   Solution: Consider the Inductive Step, where we want to prove that n-cents postage can be achieved using only 2-cent and 5-cent stamps. It would be particularly easy to prove this statement if we could assume that we can make postage of $n-2$ cents. We could then simply add a 2-cent stamp to make n-cents postage. If we use the Strong Form of Mathematical Induction, we can assume the truth of the statement for all $k < n$. In particular, we can assume the truth of the statement for $k = n-2$.

   First note that four and five cent postage can be made using 2-cent and 5-cent stamps. Stating with 6, we can use the $n-2$-th step from induction.

HW5 NEXT PAGE

HW5 DUE WEDNESDAY 10/25 BY 3pm

Problems from the books by Raji (Number Theory) and Johnsonbaugh (Discrete Mathematics).

1. Show that postage of 24 cents or more can be achieved by using only 5-cent and 7-cent stamps.

2. The Egyptians of antiquity expressed a fraction as a sum of fractions whose numerators were 1. For example, 5/6 might be expressed as

$$\frac{5}{6} = \frac{1}{2} + \frac{1}{3}. \tag{1}$$

We say that a fraction p/q, where p and q are positive integers, is in Egyptian form if

$$\frac{p}{q} = \frac{1}{n_1} + \frac{1}{n_2} + ... + \frac{1}{n_k} \tag{2}$$

where $n_1, n_2, ..., n_k$ are positive integers satisfying $n_1 < n_2 < ..... < n_k$.

   (a) Show that the representation (1) is not unique. That is, find another way to write 5/6 using fractions with numerator 1 and distinct denominators.

   (b) (NOT FOR TURNING IN, BUT COULD SHOW UP IN TEST) Prove by yourself or read the proof in Johnsonbaugh's book or any of the dozens of websites and papers on Egyptian fractions that every fraction p/q such that $0 < p/q < 1$ can be expressed in Egyptian fraction form.

   (c) Prove (using strong or complete induction *as well as* standard or weak induction) that 1 can be written in Egyptian form using k fractions with numerator 1 for *any* natural number $k \geq 3$. For example,

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = \frac{1}{2} + \frac{1}{3} + \frac{1}{9} + \frac{1}{18} = ...$$

   (d) Using the previous two results show that any nonzero rational number $r \leq 1$ can be written as a sum of unit fractions in Egyptian form in an infinite number of ways.

3. The following concern the famous Fibonacci numbers given by $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, ..., F_n = F_{n-1} + F_{n-2}....$ They are ubiquitous in nature and are related to the golden ratio, among other things.

   (a) Show that for any natural number m, F_{3m-2} and F_{3m-1} are odd while F_{3m} is even. For example, F_1 and F_2 are odd while F_3 is even.

(b) Show that for any natural number $n \geq 4$, we have

$$\left(\frac{8}{5}\right)^{n-2} < F_n < \left(\frac{9}{5}\right)^{n-2}.$$

[FYI: By the way, the golden ratio ϕ is 1.618... and it is between 8/5 and 9/5. It can be proved that $F_n/F_{n-1} \to \phi = 1.618...$ as $n \to \infty$].

4. (Binary expansion of natural numbers) Prove that every positive integer n can be represented uniquely as a sum of distinct powers of 2, i.e., in the form $n = 2^{i_0}+2^{i_1}+...2^{i_k}$ with integers $0 \leq i_0 < i_1 < i_2 < .... < i_k$.

Example: $20 = 16 + 4 = 2^4 + 2^2$. This is unique, i.e, the only way you can write 20 as a sum of *distinct powers* of 2. If you use 2 or 8 you will have to repeat one of them.