250 Homework #3

Sean O'Dea *

November 2, 2023

P3.1.4 [15 pts]

The least common multiple of two naturals x and y is the *smallest* natural that both x and y divide. For example, $lcm(8, 12) = 24$ because 8 and 12 each divide 24, and there is no smaller natural that both 8 and 12 divide.

(a) Find the least common multiple of 60 and 339.

(b) Find the least common multiple of $2^3 \cdot 3^2 \cdot 5^4$ and $2^2 \cdot 3^4 \cdot 5^3$.

(c) Describe a general method to find the least common multiple of two naturals, given their factorization into primes (and assuming that the factorization exists and is unique).

Solution:

(a)
$$\begin{aligned} 60 &= 2 \cdot 2 \cdot 3 \cdot 5 \\ 339 &= \quad 3 \cdot \quad 113 \\ \text{LCM} &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 113 = 6780 \end{aligned}$$

(b)
$$\begin{aligned} & 2^3 \cdot 3^2 \cdot 5^4 \\ & 2^2 \cdot 3^4 \cdot 5^3 \\ \text{LCM} &= 2^3 \cdot 3^4 \cdot 5^4 = 405000 \end{aligned}$$

(c) The first step is to reduce the two numbers into a prime factorization. Then you mix the prime factorizations into a compositional product that contains both of them fully. In other words, take the product of each unique factor in either factorization to the maximum power that it occurs between both factorizations. This will yield the smallest possible number that both numbers can divide.

*Collaborated with Jonah Willers.

P3.3.4 [15 pts]

We have defined the **factorial** $n!$ of a natural n to be the product of all the naturals from 1 through n, with 0! being defined as 1. Let p be an odd prime number. Prove that $(p-1)!$ is congruent to -1 modulo p. (**Hint:** Pair as many numbers as you can with their multiplicative inverses.)

Solution:

The factorial of $(p-1)$ can be defined as $1*2*3*\ldots*(p-1)$. p is a prime and all numbers in the range 1 to $p-1$ are less than p so they are all relatively prime to p, meaning they all have a multiplicative inverse (mod p). The inverse for each number in the range either already exists in the range, or can be put in the range by subtraction because it will retain its congruence class. The product of any of these pairs (mod p) will be 1.

The only numbers then that will contribute to our product are ones whose inverse is itself. By this we can express (assume x is in our factorial range):

$$x^2 \equiv 1 \text{ (mod p)}$$

By further manipulation:

$$x^2 - 1 \equiv 0 \text{ (mod p)}$$

$$(x+1)(x-1) \equiv 0 \text{ (mod p)}$$

p is prime and thus its only two divisors here can be $x+1$ or $x-1$. Using this we can say:

$$x+1 \equiv 0 \text{ (mod p) or } x-1 \equiv 0 \text{ (mod p)}$$

$$x \equiv -1 \text{ (mod p) or } x \equiv 1 \text{ (mod p)}$$

The only valid values for x in our range are 1 and $p-1$ because their inverses are themselves mod p. These two values contribute to the product while all the others between are effectively equal to 1. We can finally express:

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \text{ (mod p)}$$

$$(p-1)! \equiv p-1 \text{ (mod p)}$$

$$(p-1)! \equiv -1 \text{ (mod p)}$$

*Note: We can drop the p on the right side because of the congruency class over p.

P3.5.4 [17 pts]

Suppose that the naturals $m_1, \ldots, m_k$ are pairwise relatively prime and that for each i from 1 through k, the natural x satisfies $x \equiv x_i \pmod{m_i}$ and the natural y satisfies $y \equiv y_i \pmod{m_i}$. Explain why for each i, xy satisfies $xy \equiv x_i y_i \pmod{m_i}$ and $x + y$ satisfies $(x + y) \equiv (x_i + y_i) \pmod{m_i}$. Now suppose that $z_1, \ldots, z_j$ are some naturals and that we have an arithmetic expression in the z_i's (a combination of them using sums and products) whose result is guaranteed to be less than M, the product of the m_i's. Explain how we can compute the exact result of this arithmetic expression using the Chinese Remainder Theorem only once, no matter how large j is.

Solution:

$xy \equiv x_i y_i \pmod{m_i}$:

Because $x \equiv x_i \pmod{m_i}$ and $y \equiv y_i \pmod{m_i}$, we can express them as:

$$x = x_i + m_i a$$

$$y = y_i + m_i b$$

Where a and b are two arbitrary naturals. This now means:

$$xy = (x_i + m_i a)(y_i + m_i b)$$

$$xy = x_i y_i + x_i m_i b + m_i a y_i + {m_i}^2 ab$$

Dividing by m_i will eliminate all terms on the right besides $x_i y_i$, so:

$$xy \equiv x_i y_i \pmod{\text{mi}}$$

$x + y \equiv (x_i + y_i) \pmod{m_i}$:

Using the same expressions from above:

$$x = x_i + m_i a$$

$$y = y_i + m_i b$$

Now combining:

$$x + y = x_i + y_i + m_i a + m_i b$$

The two terms on the far right will factor out when dividing by m_i:

$$x + y \equiv x_i + y_i$$

P4.1.6 [8 pts]

(Uses Java) Give a recursive definition of and a recursive static method for the **natural subtraction** function, with pseudo-Java header

`natural minus (natural x, natural y).`

On input x and y this function returns $x-y$ if this is a natural (i.e., if $x \geq y$) and 0 otherwise.

Solution:

```
public static natural minus (natural x, natural y) {
   if (x < y) return 0;
   if (isZero(y)) return x;
   return pred(minus(x, pred(y)));
}
```

Note:

- boolean isZero(natural x) returns true if and only if x is equal to zero.
- natural pred(natural x) returns the predecessor of a given natural.

P4.3.2 [15 pts]

Let the finite sequence $a_0, a_1, \ldots, a_n$ be defined by the rule $a_i = b + i \cdot c$. Prove by induction on n that the sum of the terms in the sequence is $(n+1)(a_0 + a_n)/2$. (**Hint:** In the base case, $n = 0$ and so a_0 is equal to a_n. For the induction case, note that the sum for $n+1$ is equal to the sum for n plus the one new term $a_n + 1$.)

Solution:

The sum of the sequence can be represented by S(n).

$$S(n) = \sum_{i=0}^{n} b+ci \text{ ; } a_0 = b, \; a_n = b+cn \text{ so } \frac{(n+1)(a_0 + a_n)}{2} = \frac{(n+1)(b+b+cn)}{2} = \frac{(n+1)(2b+cn)}{2}$$

Base Case: When $n = 0$, $S(0) = b$ and $\dfrac{(0+1)(2b+c(0))}{2} = b$, so $b = b$.

Inductive Hypothesis: Assume $S(k) = \dfrac{(k+1)(2b+ck)}{2}$ for some arbitrary natural k.

Inductive Step:

$$S(k+1) = S(k) + a_{n+1} = S(k) + b + c(k+1) = S(k) + b + ck + c \text{ (LHS)}$$

$$S(k) = \frac{(k+1)(2b+ck)}{2} = \frac{2bk + 2b + ck^2 + ck}{2}$$

$$\text{(Substitute k+1 into RHS)} \frac{((k+1)+1)(2b+c(k+1))}{2} = \frac{(k+2)(2b+ck+c)}{2}$$

$$= \frac{2bk + ck^2 + ck + 4b + 2ck + 2c}{2} = \frac{2bk + 2b + ck^2 + ck}{2} + \frac{2b + 2ck + 2c}{2}$$

$$= \frac{2bk + 2b + ck^2 + ck}{2} + b + ck + c = S(k) + bck + c \text{ (RHS)}$$

RHS = LHS, thus the sum of the terms in the sequence can be represented by $(n+1)(a_0 + a_n)/2$.

P4.3.6 [15 pts]

Define $S(n)$ to be the sum, for all i from 1 through n, of $\frac{1}{i(i+1)}$. Prove by induction on all naturals n (including 0) that $S(n) = 1 - \frac{1}{n+1}$.

Solution:

$$S(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{1}{1(1+1)} \frac{1}{2(2+1)} + \ldots + \frac{1}{n(n+1)}$$

Base Case: When $n = 0$, $S(0) = 0 = 1 - \dfrac{1}{0+1}$, or, $0 = 0$

Inductive Hypothesis: Assume $S(k) = 1 - \dfrac{1}{k+1}$ for some arbitrary natural k.

Inductive Step:

$$S(k+1) = S(k) + \frac{1}{(k+1)((k+1)+1)} = S(k) + \frac{1}{(k+1)(k+2)} \text{ (LHS)}$$

$$1 - \frac{1}{k+1} = \frac{k+1-1}{k+1} = \frac{k}{k+1} \text{ (Now substitute k+1)}$$

$$\frac{(k+1)}{(k+1)+1} = \frac{k+1}{k+2} = \frac{(k+1)(k+1)}{(k+1)(k+2)} = \frac{k^2+2k+1}{(k+1)(k+2)}$$

$$= \frac{k^2+2k}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)} = \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = (1 - \frac{1}{k+1}) + \frac{1}{(k+1)(k+2)} \text{ (From earlier conclusion)}$$

$$= S(k) + \frac{1}{(k+1)(k+2)} \text{ (RHS)}$$

RHS = LHS, thus $S(n) = 1 - \frac{1}{n+1}$ for all naturals.

P4.4.1 [15 pts]

Consider a variant of Exercise 4.4.3, for \$4 and \$11 bills (made, we might suppose, by a particularly inept counterfeiter). What is the minimum number k such that you can make up \$n for all $n \geq k$? Prove that you can do so.

Solution:

The minimum number k such that you can make up \$n for all $n \geq k$ is \$30.

Proof by Induction:

Base Case: 29 cannot be made as a linear combination of 4 and 11, so we cannot use 29 (or any previous natural). Let's consider 30 which can be written as $30 = 11 + 11 + 4 + 4$. This will be our base case.

Inductive Hypothesis: Let's assume for some arbitrary $k \geq 30$ the amount of k dollars can be made as a combination of \$4 and \$11 bills.

Inductive Step: Let's consider two cases.

- We use at least one \$11 bill to reach k.
  In this case we replace one of the \$11 bills with four \$3 bills. $(k - 11) + (4 * 3) = k + 1$
- We don't use any \$11 bills to reach k.
  In this case all of the bills are \$4 and since $k \geq 30$ we have at least eight of them. We can replace eight of the \$4 bills with three \$11 bills. $(k - (4 * 8)) + (11 * 3) = k + 1$

In both cases the proceeding natural can be reached and thus all values $n \geq 30$.

EC: P3.4.6 [10 pts]

A **Fermat number** is a natural of the form $F_i = 2^{2^i} + 1$, where i is any natural. In 1730 Goldbach used Fermat numbers to give an alternate proof that there are infinitely many primes.

(a) List the Fermat numbers F_0, F_1, F_2, F_3, and F_4.

(b) Prove that for any n, the product $F_0 \cdot F_1 \cdot \ldots \cdot F_n$ is equal to $F_{n+1} - 2$.

(c) Argue that no two different Fermat numbers can share a prime factor. Since there are infinitely many Fermat numbers, there must thus be infinitely many primes.

Solution:

(a)
- $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$
- $F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$
- $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$
- $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$
- $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65537$