COMPSCI 250: Fall 2023
Homework 3

David A. Mix Barrington , Ghazaleh Parvini

Due Date : Friday, October 20

(15 points) **Problem 3.1.4**

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 $2^3 3^2 5^4$ and $2^2 3^4 5^3$.

(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) Since $60 = 2 * 2 * 3 * 5$ and $339 = 3 * 113$, the method below gives $2 * 2 * 3 * 5 * 113 = 6780$.

(b) A number is a multiple of $2^i \cdot 3^j \cdot 5^k$ if the exponents of 2, 3, and 5 in its factorization are $\geq i$, j, and k respectively. So the least common multiple has exponents for each prime that are the maximum of the exponents of that prime in the two input numbers. In this case, the least common multiple is $2^3 \cdot 3^4 \cdot 5^4$.

(c) Factor each of the two input numbers into primes. For each prime that occurs in either, choose the maximum of the two exponents. The least common multiple is the product of the prime powers given by taking each prime and raising it to the maximum exponent.

(15 points) **Problem 3.3.4**

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:

Since p is odd, the product $1 \cdot 2 \cdots (p-1)$ contains an even number of terms. Since p is prime, each number from 1 to $p-1$ is relatively prime to p and thus has an inverse mod p.

We can pair off each number with its inverse, removing both numbers from the product. However, some numbers are their own inverse. This happens when

$$\begin{aligned} x^2 &\equiv 1 \mod p \\ x^2 - 1 &\equiv 0 \mod p \\ (x+1)(x-1) &\equiv 0 \mod p \end{aligned}$$

Since all numbers from 1 to $p-1$ are relatively prime to p, the product of any two non-zero numbers in the range is never $0 \mod p$. Thus x is its own inverse when $x+1 \equiv 0 \mod p$) or $x - 1 \equiv 0 \mod p$.This gives $x \equiv -1 \mod p$ or $x \equiv 1 \mod p$. Now we can remove all terms from the product except 1 and $p-1$.

$$\begin{aligned} (p-1)! \equiv & 1 \cdot 2 \cdots (p-1) \mod p & (1) \\ \equiv & 1 \cdot (p-1) \mod p & (2) \\ \equiv & -1 \mod p & (3) \end{aligned}$$

(17 points) **Problem 3.5.4**

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 $z_1, \cdots, z_j$ 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:

We know that for each m_i, $x = x_i \pmod{m_i}$ and $y = y_i \pmod{m_i}$. Our sum and product rules for congruences modulo a single base tell us that $xy = x_i y_i \pmod{m_i}$ and $x + y = x_i + y_i \pmod{m_i}$.

Given the arithmetic expression in the z's, repeated application of the sum and product rules tell us that the result r of the expression is congruent, modulo each m_i, to the result of the same sum and products on the m_i remainder of the z's. For each m_i, let r_i be the result of this arithmetic modulo m_i.

Once we have all of these r_i's, the Chinese Remainder Theorem (in its full form) gives us a number that is congruent to r modulo M. If we know that r is actually between 0 and $M-1$, there is only one number in this range that is congruent to our number modulo M, so this number must be r.

(8 points) **Problem 4.1.6**

(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:

```
natural minus (natural x, natural y) {
  if (y > x) {
    return 0;
  } else if (y == 0) {
    return x;
  } else {
    return minus(pred(x), pred(y));
  }
}
```

(15 points) **Problem 4.3.2**

Let the finite sequence $a_0, a_1, \cdots, a_n$ 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:

$S(n) = \sum_{i=0}^{n} a_i$

$P(n) : S(n) = \frac{(n+1)(a_0+a_n)}{2}$

Base Case: $n = 0$. $S(0) = a_0$

Inductive Hypothesis: For any number n, $S(n) = \frac{(n+1)(a_0+a_n)}{2}$

Inductive Hypothesis: For $(n+1)$:

$$\begin{aligned}
S(n+1) &= S(n) + a_{n+1} \\
&= \frac{(n+1)(a_0 + a_n)}{2} + b + (n+1)c \\
&= \frac{(n+1)(b+b+nc) + 2b + 2(n+1)c}{2} \\
&= \frac{(n+1+1)(b+b+nc) + (n+2)c}{2} \\
&= \frac{(n+1+1)(b+b+(n+1)c)}{2} \\
&= \frac{(n+1+1)(a_0 + a_{n+1})}{2}
\end{aligned}$$

(15 points) **Problem 4.3.6**

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:

Let $P(n)$ be the statement:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}$$

First, we have to show that the base case, $P(0)$, is true,

$$\sum_{i=1}^{0} \frac{1}{i(i+1)} \stackrel{?}{=} 1 - \frac{1}{0+1}$$

$$0 = 1 - 1$$

Now that we've shown the base case is true, we have to show that $P(n) \implies P(n+1)$. If $P(n)$ is false, $P(n) \implies P(n+1)$ is vacuously true. Now, let's assume that $P(n)$ is true.

$P(n+1)$ is the statement:

$$\sum_{i=1}^{n+1} \frac{1}{i(i+1)} = 1 - \frac{1}{(n+1)+1}$$

And we've assumed that:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{(n)+1}$$

So we can replace the first n terms of the summation with this formula, and proceed with a

bit of algebra:

$$1 - \frac{1}{n+1} + \sum_{i=n}^{n+1} \frac{1}{i(i+1)} \stackrel{?}{=} 1 - \frac{1}{(n+1)+1}$$
$$1 - \frac{1}{n+1} + \frac{1}{(n+1)((n+1)+1)} \stackrel{?}{=} 1 - \frac{1}{n+2}$$
$$1 - \frac{1}{n+1} * \frac{n+2}{n+2} + \frac{1}{(n+1)(n+2)} \stackrel{?}{=} 1 - \frac{1}{n+2}$$
$$1 - \frac{n+2}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \stackrel{?}{=} 1 - \frac{1}{n+2}$$
$$1 - \frac{n+1}{(n+1)(n+2)} \stackrel{?}{=} 1 - \frac{1}{n+2}$$
$$1 - \frac{1}{n+2} = 1 - \frac{1}{n+2}$$

Because we've shown $P(0)$ and $P(n) \implies P(n+1)$, we can conclude $\forall x : P(x)$, and our proof by induction is complete.

(15 points) **Problem 4.4.1**

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:

$k = 30$
Base Case: $30 = 2 \times \$4 + 2 \times \$11$
Let $Q(n)$ be the statement, for all i such that $30 \leq i \leq n$, i can be made up of only \$4 and \$11 bills.
Inductive hypothesis: Assume $Q(n)$ to be true.
Inductive Step: Prove $Q(n+1)$: Proof by Cases:

Case 1: n is made of at least one \$11 bill
$Q(n+1)$ will be true because an \$11 bill can be replaced with 3 \$4 bills, incrementing the sum by \$1.

Case 2: n dollars is not made of any \$11 bills
It must be made of at least 8 \$4 bills ($n = 31 = 5 \times \$4 + 1 \times \$11$ and $n = 32 = 8 \times \$4$). 8 \$4 bills can be replaced with 3 \$11 bills, increasing the sum by 1.

Extra credit:

(10 points) **Problem 3.4.6**

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 $F_0 \cdot F_1 \cdot ... \cdot F_n$ 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) $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, and $F_4 = 2^{16} + 1 = 65537$.

(b) By ordinary induction on n. For the base case, $F_0 = 3 = F_1 - 2 = 5 - 2$. Let $P(n)$ be the product $F_0 \cdot \ldots F_n$. Assume for the IH that $P(n) = F_{n+1} - 2$. Then $P(n+1) = P(n) \cdot F_{n+1} = (F_{n+1} - 2)F_{n+1} = (2^{2^{n+1}} - 1)(2^{2^{n+1}} + 1) = 2^{2^{n+2}} - 1 = F_{n+2} - 2$. This proves the IG and completes the induction.

(c) Let F_i and F_j be any two Fermat numbers, with $i < j$. Then F_j is congruent to -2 modulo a product that contains F_i, so it is also congruent to -2 modulo F_i itself. Since F_i is an odd prime, -2 is not congruent to 0 modulo F_i. Thus F_j is not divisible by F_i. Hence no two Fermat numbers can share a prime factor.