# Math 124 Homework 1 Solutions

by Luke Gustafson

Fall 2003

**1.**

$$64 = 2 \cdot 28 + 8$$
$$28 = 3 \cdot 8 + 4$$
$$8 = 2 \cdot 4$$

Hence, $\gcd(64, 28) = 4$.

$$119 = 2 \cdot 49 + 21$$
$$49 = 2 \cdot 21 + 7$$
$$21 = 3 \cdot 7$$

Hence, $\gcd(119, 49) = 7$.

$$144 = 89 + 55$$
$$89 = 55 + 34$$
$$55 = 34 + 21$$
$$34 = 21 + 13$$
$$21 = 13 + 8$$
$$13 = 8 + 5$$
$$8 = 5 + 3$$
$$5 = 3 + 2$$
$$3 = 2 + 1$$
$$2 = 2 \cdot 1$$

Hence, $\gcd(144, 89) = 1$.

**2a.** We must have $q_1 \geq 1$, so $a_0 \geq a_1 + a_2$. Thus

$$a_0 + \phi a_1 \geq a_1 + a_2 + \phi a_1$$
$$a_0 + \phi a_1 \geq a_1 + \phi a_1 + \phi a_2 + \phi^2 a_2$$

$$a_0 + \phi a_1 \geq (1+\phi)(a_1 + \phi a_2)$$

**2b.** The hypotheses of the previous problem match the conditions of the Euclidean Algorithm. Therefore, at each step of the Euclidean Algorithm $a_i = q_{i+1}a_{i+1} + a_{i+2}$ we have the inequality $a_i + \phi a_{i+1} \geq (1+\phi)(a_{i+1} + \phi a_{i+2})$. Multiply together this inequality for $i = 0$ to $i = k$ and cancel all the common factors to get

$$a_0 + \phi a_1 \geq (1+\phi)^{k+1}(a_{k+1} + \phi a_{k+2})$$

Since $a_0$ and $a_1$ are at most $10^{10^9}$, $a_0 + \phi a_1$ is at most $10^{10^9}(1+\phi)$. Plugging that into the previous inequality, we obtain

$$10^{10^9}(1+\phi) \geq (1+\phi)^{k+1}(a_{k+1} + \phi a_{k+2})$$

$$\frac{10^{10^9}}{(1+\phi)^k} \geq a_{k+1} + \phi a_{k+2}$$

Note that the Euclidean Algorithm must have terminated after $k$ steps if $a_{k+1} = 0$. So, if $a_{k+1} + \phi a_{k+2}$ is less than one for some $k$, then the algorithm has terminated. Let us determine when this is the case:

$$1 > \frac{10^{10^9}}{(1+\phi)^k}$$

Taking logs of both sides, we get

$$0 > 10^9 \log 10 - k \log(1+\phi)$$

$$k > \frac{10^9 \log 10}{\log(1+\phi)}$$

The right side evaluates to 4,784,971,966+, so $k = 4{,}784{,}971{,}967$ works, and the algorithm must terminate in less than 5 billion steps.

**3.** First, divide by the common factor to obtain the equivalent equation $16x + 7y = 3$. We first find a solution to $16x + 7y = 1$ using the Euclidean Algorithm.

$$16 = 2 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

Therefore

$$1 = 7 - 3 \cdot 2$$

$$1 = 7 - 3(16 - 2 \cdot 7)$$

$$1 = 7 \cdot 7 - 3 \cdot 16$$

which gives us the solution $(x, y) = (-3, 7)$. Multiply this by 3 to get a solution to the original equation: $(x, y) = (-9, 21)$. Finally, this gives us the general solution $(x, y) = (-9 + 7k, 21 - 16k)$, $k \in \mathbb{Z}$.

**4.** First, we solve the first two equations, $x \equiv 5 \pmod 7$ and $x \equiv 7 \pmod{11}$. From the first equation, we get $x = 5+7y$ for some $y \in \mathbb{Z}$. Substitute this into the second equation to get $5+7y \equiv 7 \pmod{11}$, which means $5+7y = 7+11z$ for some $z \in \mathbb{Z}$. Solving this equation, we find a solution $(y, z) = (-6, -4)$. So, $x = 5 + 7 \cdot -6 = -37$ is a solution $\pmod{77}$.

Therefore, the first two equations are equivalent to the single equation $x \equiv -37 \pmod{77}$. Next, we solve this equation and $x \equiv 11 \pmod{13}$. From the first equation, we have $x = -37 + 77y$ for some $y \in \mathbb{Z}$. Substitute to get $-37+77y \equiv 11 \pmod{13}$. Reduce this to $2-y \equiv 11 \pmod{13}$, which means $2 - y = 11 + 13z$ for some $z \in \mathbb{Z}$. Solving this equation, we find a solution $(y, z) = (-9, 0)$. So, $x = -37 + 77 \cdot -9 = -730$.

Therefore, the general solution to all three equations is $x \equiv -730 \pmod{1001}$. This gives positive solutions $271, 1272, 2273, \ldots$, and the second smallest positive solution is 1272.

**5.** There are numerous possibilities. Some of the simpler ones include:
$x^3 - x \pmod 6$, which has zeroes 0, 1, 2, 3, 4, and 5
$x^2 - 1 \pmod 8$, which has zeroes 1, 3, 5, and 7
$x^2 \pmod{16}$, which has zeroes 0, 4, 8, and 12

**6.** Recall from class $\varphi(p_1^{e_1}p_2^{e_2}\cdots) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\cdots$. Now, if $\varphi(n) = 2$, then each of the factors $p_i^{e_i-1}(p_i-1)$ must be either one or two. Let's look at the possibilities for these factors.

First, if $p_i > 3$, then $p_i - 1 > 2$, so $p_i^{e_i-1}(p_i-1) > 2$. That leaves the cases $p_i = 2$ and $p_i = 3$.

If $p_i = 2$, then $p_i^{e_i-1}(p_i-1) = 2^{e_i-1}$, so $e_i = 1$ or $e_i = 2$.

If $p_i = 3$, then $p_i^{e_i-1}(p_i-1) = 2 \cdot 3^{e_i-1}$. Then we must have $e_i = 1$.

So the prime powers dividing $n$ can only be $2^1$, $2^2$, or $3^1$. Hence we only need to look at $n \le 2^2 \cdot 3^1 = 12$, and specifically $n = 1, 2, 3, 4, 6, 12$. We find that $n = 3$, 4, and 6 are all the solutions to $\varphi(n) = 2$.