

MATH221-001 200530 Problem Set 1 Solutions

Edward Doolittle

Friday, September 30, 2005

1. $100 - 23 = 77$; $77 - 23 = 54$; $54 - 23 = 31$; $31 - 23 = 8$; and 8 is less than 23 so we are finished. Putting those equations back together we see that $100 = 23 + 77 = 23 + 23 + 54 = 23 + 23 + 23 + 31 = 23 + 23 + 23 + 23 + 8 = 23 \times 4 + 8$ which gives the required representation of 100, i.e., $100 = 23q + r$ where $q = 4$ and $r = 8$.
2. By the standard long division algorithm (or by using a calculator in the way I showed you during the lectures),

$$\begin{array}{r} 35 \text{ R } 21 \\ \text{-----} \\ 28 \overline{)1001} \\ \underline{84} \\ \underline{161} \\ \underline{140} \\ \text{---} \\ 21 \end{array}$$

which gives $q = 35$ and $r = 21$. You should check that the q and r you have obtained actually does satisfy the requirements $1001 = 28 \times 35 + 21$ and $0 \leq 21 < 28$.

3. We first find the representation of 2005 in base 16 by repeated division of remainders by 16:

$$\begin{array}{r} 125 \text{ R } 5 \\ \text{-----} \\ 16 \overline{)2005} \\ \underline{16} \\ \underline{40} \\ \underline{32} \\ \text{---} \\ 85 \\ \underline{80} \\ \text{---} \\ 5 \end{array} \qquad \begin{array}{r} 7 \text{ R } 13 \\ \text{-----} \\ 16 \overline{)125} \\ \underline{112} \\ \underline{13} \end{array} \qquad \begin{array}{r} 0 \text{ R } 7 \\ \text{---} \\ 16 \overline{)7} \end{array}$$

so $2005 = 7 \times 16^2 + 13 \times 16^1 + 5 \times 16^0$. (You should check that by performing the arithmetic.) The conventional representation for that in base 16 notation is $(7D5)_{16}$, where the D is a single digit which stands for 13. (If you wrote $(7 \ 13 \ 5)_{16}$, preferably with some space or some other delimiter between the 7 and 1 and between the 3 and 5, that is acceptable too for now.)

The base 2 representation can be found by the same method. However, there is a shortcut that can be used to convert base 16 to base 2: $(7)_{16} = (0111)_2$, $(D)_{16} = (1101)_2$, and $(5)_{16} = 0101_2$, so just concatenating those results,

$$(7D5)_{16} = (0111, 1101, 0101)_2$$

Note that this short cut only works for a few pairs of bases and won't help you convert from one base to another in general.

4. Repeatedly dividing,

$$\begin{array}{r}
 5 \text{ R } 924 \\
 \hline
 6930 \overline{)35574} \\
 \underline{34650} \\
 924
 \end{array}
 \qquad
 \begin{array}{r}
 7 \text{ R } 462 \\
 \hline
 924 \overline{)6930} \\
 \underline{462} \\
 462
 \end{array}
 \qquad
 \begin{array}{r}
 2 \text{ R } 0 \\
 \hline
 462 \overline{)924} \\
 \underline{924} \\
 0
 \end{array}$$

so $\gcd(6930, 35574) = 462$.

5. First we use the Euclidean algorithm to find the gcd of 1001 and 288:

$$\begin{array}{r}
 3 \text{ R } 137 \\
 \hline
 288 \overline{)1001} \\
 \underline{864} \\
 137
 \end{array}
 \qquad
 \begin{array}{r}
 2 \text{ R } 14 \\
 \hline
 137 \overline{)288} \\
 \underline{274} \\
 14
 \end{array}
 \qquad
 \begin{array}{r}
 9 \text{ R } 11 \\
 \hline
 14 \overline{)137} \\
 \underline{126} \\
 11
 \end{array}
 \qquad
 \begin{array}{r}
 1 \text{ R } 3 \\
 \hline
 11 \overline{)14} \\
 \underline{11} \\
 3
 \end{array}
 \qquad
 \begin{array}{r}
 3 \text{ R } 2 \\
 \hline
 3 \overline{)11} \\
 \underline{9} \\
 2
 \end{array}
 \qquad
 \begin{array}{r}
 1 \text{ R } 1 \\
 \hline
 2 \overline{)3} \\
 \underline{2} \\
 1
 \end{array}$$

so $\gcd(288, 1001) = 1$. But using the “division equation” we can also write

$$1 = 3 \times 1 - 2 \times 1 \tag{1}$$

$$2 = 11 \times 1 - 3 \times 3 \tag{2}$$

$$3 = 14 \times 1 - 11 \times 1 \tag{3}$$

$$11 = 137 \times 1 - 14 \times 9 \tag{4}$$

$$14 = 288 \times 1 - 137 \times 2 \tag{5}$$

$$137 = 1001 \times 1 - 288 \times 3. \tag{6}$$

Substituting equation 2 into equation 1,

$$\begin{aligned}
 1 &= 3 \times 1 - (11 \times 1 - 3 \times 3) \\
 &= 3 \times 1 + 3 \times 3 - 11 \times 1 \\
 &= 3 \times 4 - 11 \times 1
 \end{aligned}$$

Now substituting equation 3 into the above,

$$\begin{aligned}
 1 &= (14 \times 1 - 11 \times 1) \times 4 - 11 \times 1 \\
 &= 14 \times 4 - 11 \times 4 - 11 \times 1 \\
 &= 14 \times 4 - 11 \times 5.
 \end{aligned}$$

Substituting equation 4 into the above,

$$\begin{aligned}
 1 &= 14 \times 4 - (137 \times 1 - 14 \times 9) \times 5 \\
 &= 14 \times 4 - 137 \times 5 + 14 \times 45 \\
 &= 14 \times 49 - 137 \times 5.
 \end{aligned}$$

Substituting equation 5 into the above,

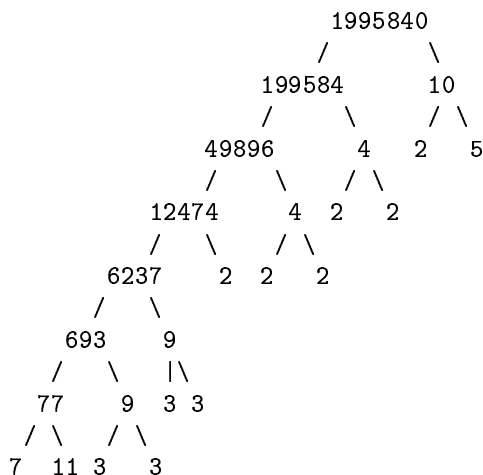
$$\begin{aligned}
 1 &= (288 \times 1 - 137 \times 2) \times 49 - 137 \times 5 \\
 &= 288 \times 49 - 137 \times 98 - 137 \times 5 \\
 &= 288 \times 49 - 137 \times 103.
 \end{aligned}$$

Finally, substituting equation 6 into the above,

$$\begin{aligned} 1 &= 288 \times 49 - (1001 \times 1 - 288 \times 3) \times 103 \\ &= 288 \times 49 - 1001 \times 103 + 288 \times 309 \\ &= 288 \times 358 - 1001 \times 103, \end{aligned}$$

which gives an answer to the question: $m = -103$ and $n = 358$. (You should check that those values of m and n actually do work.)

6. According to the factor tree:



the answer is $1995840 = 2^6 \times 3^4 \times 5^1 \times 7^1 \times 11^1$. (There are many ways of building the factor tree, but there is only one prime factorization.)

7. You could use the unique factorization theorem to answer this question, which is the way most people would do it. Below, I have written two other possible ways you could answer this question. In both cases, it will help you understand if you pick a few different values of a , b , and m and follow along with the arguments. The second method is a quite unusual, but it may be more understandable, and it works.

(a) Let $D = \gcd(ma, mb)$. Since D is a common divisor of ma and mb we can write $ma = rD$ and $mb = sD$. Also, by the Euclidean algorithm, D can be written $D = pma + qmb = m(pa + qb)$ for some p and q , which shows that D is divisible by m , and means that we can write $D = mD_1$ for some integer D_1 . Then $ma = rmD_1$ and $mb = smD_1$. Dividing through by m gives $a = rD_1$ and $b = sD_1$, which shows that D_1 is a common divisor of a and b . Then the largest possible value for D_1 is $\gcd(a, b)$, so the largest possible value for D is $m \gcd(a, b)$. On the other hand, $m \gcd(a, b)$ really is a common divisor of ma and mb .

To summarize, $m \gcd(a, b)$ is a common divisor of ma and mb , and no larger integer can be a common divisor of ma and mb , which means that $m \gcd(a, b) = \gcd(ma, mb)$.

(b) *Analysis:* Let's pick some values of a , b , and m and apply the Euclidean algorithm to find $\gcd(a, b)$ and apply the Euclidean algorithm to find $\gcd(ma, mb)$. For example, let $a = 9$, $b = 15$, and $m = 2$. (You should pick your own a , b , and m and follow along.)

$$\begin{array}{r} 1 \text{ R } 6 \\ \text{---} \\ 9 \overline{)15} \\ \underline{9} \\ - \\ 6 \end{array} \qquad \begin{array}{r} 1 \text{ R } 12 \\ \text{---} \\ 18 \overline{)30} \\ \underline{18} \\ -- \\ 12 \end{array}$$

$$\begin{array}{r}
1 \text{ R } 3 \\
\text{---} \\
6)9 \\
6 \\
- \\
3
\end{array}
\qquad
\begin{array}{r}
1 \text{ R } 6 \\
\text{---} \\
12)18 \\
12 \\
- \\
6
\end{array}$$

$$\begin{array}{r}
2 \text{ R } 0 \\
\text{---} \\
3)6 \\
6 \\
- \\
0
\end{array}
\qquad
\begin{array}{r}
2 \text{ R } 0 \\
\text{---} \\
6)12 \\
12 \\
- \\
0
\end{array}$$

Notice that the two runs of the Euclidean algorithm are closely related. One is a sort of “distorted mirror” of the other. Every number in the calculation of $\gcd(18, 30)$ is twice every number in the calculation of $\gcd(9, 15)$, with the exception of the quotients, which are the same. Try this on a few more examples, and you’ll see that in every case, the run of the algorithm for ma and mb can be obtained from the run of the algorithm for a and b by multiplying every number by m except for the quotients. That observation is good enough for full marks for now, but in order to turn it into a real, valid, mathematical proof, see the following.

Proof: Suppose $a < b$. When finding $\gcd(a, b)$, we divide b by a to obtain $b = qa + r$ where $0 \leq r < a$. Then $mb = qma + mr$ where $0 \leq mr < ma$, which is the first required operation in finding $\gcd(ma, mb)$ by the Euclidean algorithm.

The next step, when finding $\gcd(a, b)$, is to divide a by r to obtain $a = q_1r + r_1$ where $0 \leq r_1 < r$. Again multiplying through by m we obtain $ma = q_1mr + mr_1$ where $0 \leq mr_1 < mr$, which is the second required operation in finding $\gcd(ma, mb)$ by the Euclidean algorithm.

We continue in this way until we obtain a remainder of 0 in the sequence of divisions for finding $\gcd(a, b)$; say, $r_{k-1} = q_{k+1}r_k + r_{k+1}$ where $0 = r_{k+1}$. Then $\gcd(a, b) = r_k$. On the other hand, the corresponding equation for $\gcd(ma, mb)$ is $mr_{k-1} = q_{k+1}mr_k + mr_{k+1}$, which shows that $\gcd(ma, mb) = mr_k = m \gcd(a, b)$.

8. The best definition of $\gcd(a_1, a_2, \dots, a_n)$ is that it is the largest element of the set of common divisors of a_1, \dots, a_n . A second definition (which you should actually prove as a theorem if you are going to use the first definition) is

$$\gcd(a_1, a_2, \dots, a_{n-1}, a_n) = \gcd(\gcd(a_1, a_2, \dots, a_{n-1}), a_n), \quad (7)$$

in other words, to find the greatest common divisor of n numbers, find the greatest common divisor of the first $n - 1$ numbers, and then find the greatest common divisor of that result and a_n .

Using that second characterization of the greatest common divisor of n , we can prove the theorem. Let’s start by proving it for $n = 3$. By the theorem from the lectures, $\gcd(a_1, a_2) = pa_1 + qa_2$ for some integers p and q . Then

$$\begin{aligned}
\gcd(a_1, a_2, a_3) &= \gcd(\gcd(a_1, a_2), a_3) \\
&= \gcd(pa_1 + qa_2, a_3) \\
&= r(pa_1 + qa_2) + sa_3 \\
&= rpa_1 + rqa_2 + sa_3,
\end{aligned}$$

so $\gcd(a_1, a_2, a_3) = x_1a_1 + x_2a_2 + x_3a_3$ holds for $x_1 = rp$, $x_2 = rq$, and $x_3 = s$.

The process can be repeated in an obvious way for $n = 4$, $n = 5$, and so on, which proves the required theorem. (Actually, to really complete this, we need to invoke mathematical induction, but we will talk about that some other time.)

9. Let's calculate Fibonacci numbers until we find two larger than 100: $f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, f_8 = 21, f_9 = 34, f_{10} = 55, f_{11} = 89, f_{12} = 144, f_{13} = 233, \dots$. Applying the Euclidean algorithm, $\gcd(144, 233) = \gcd(144, 89) = \gcd(55, 89) = \dots = \gcd(3, 2) = \gcd(1, 2) = \gcd(1, 1)$. After a little experimenting you should see that $\gcd(f_k, f_{k+1})$ can be calculated in k divisions (or $k - 1$ or $k - 2$ divisions depending on what shortcuts you use in the last few steps). It is enough to observe that the problem for $\gcd(f_k, f_{k+1})$ can be reduced to the problem for $\gcd(f_k, f_{k-1})$ in one step, but to really finish this off, you could use an induction argument, which we will talk about later.
10. This is a very challenging problem. There are a number of different ways of attacking it depending on the tools we have at our disposal. Below I have sketched two possible approaches to solving the problem. I'm sure there are many others.
- (a) One way involves using modular arithmetic modulo 2, modulo 2^2 , modulo 2^3 , and so on to see which powers of 2 might divide which Fibonacci numbers. For example, working modulo 2 you should see a pattern odd, odd, even, odd, odd, even, etc. Working modulo 4 you should see that every sixth Fibonacci number is divisible by 4. Look again at the sequence modulo 3, modulo 3^2 , and so on, and then for any prime power modulus p^k . You should be able to figure out patterns which will help you determine the factorizations of Fibonacci numbers, and the result will follow after a little more work.
- (b) Another way of solving the problem uses the idea in solution 7b. If we can show that $\gcd(f_m, f_n) = \gcd(f_{m-n}, f_n)$ for any $m > n$ then we can run two parallel Euclidean algorithms, one to find $\gcd(f_m, f_n)$ and the other to find $\gcd(m, n)$, and obtain a mapping from one run of the algorithm to the other. So you should begin by exploring how f_{n+k} can be expressed in terms of f_{n+1} and f_n by successively writing $f_{n+k} = f_{n+k-1} + f_{n+k-2}$ and expanding each of those in turn until you arrive at an expression involving just f_{n+1} and f_n . First try for $k = 1$ (nothing to do), $k = 2$, $k = 3$, and so on. You should start to see other Fibonacci numbers appearing. The result you should eventually obtain is $f_{n+k} = f_k f_{n+1} + f_{k-1} f_n$. The proper way to prove this formula is through mathematical induction, but I am not requiring induction arguments from you at this stage.

Now let's look at $\gcd(f_{n+k}, f_n)$. According to the above formula,

$$\gcd(f_{n+k}, f_n) = \gcd(f_k f_{n+1} + f_{k-1} f_n, f_n). \quad (8)$$

Subtracting f_n from the first number f_{k-1} times, we obtain

$$\gcd(f_k f_{n+1} + f_{k-1} f_n, f_n) = \gcd(f_k f_{n+1}, f_n). \quad (9)$$

However, by an earlier problem in the textbook, f_{n+1} and f_n have no common factor, so

$$\gcd(f_k f_{n+1}, f_n) = \gcd(f_k, f_n). \quad (10)$$

Putting it all together and letting $k = m - n$ we see that $\gcd(f_m, f_n) = \gcd(f_{m-n}, f_n)$. Now we can run parallel Euclidean algorithms in the style of solution 7b.