

MATH221-001 200530 Term Test 1 Solutions

Edward Doolittle

October 18, 2005

1. (2 marks) Find numbers q and r such that $378 = 322q + r$, $0 \leq r < 322$.

By long division, or alternatively by using a calculator in the way I discussed in the lectures,

$$\begin{array}{r} 1 \text{ R } 56 \\ \text{----} \\ 322 \overline{)378} \\ \underline{322} \\ 56 \end{array}$$

So $378 = 322q + r$ where $q = 1$ and $r = 56$.

2. (3 marks) Find the greatest common divisor of 378 and 322.

The gcd can be found using the Euclidean algorithm. By the previous problem,

$$378 = 322 \times 1 + 56.$$

Dividing 322 by 56, etc., gives

$$322 = 56 \times 5 + 42$$

$$56 = 42 \times 1 + 14$$

$$42 = 14 \times 3 + 0$$

We stop when the remainder is 0. The divisor in the last equation is the gcd, so $\gcd(378, 322) = 14$.

3. (5 marks) Find integers m and n such that $378m + 322n = 28$.

Re-writing the above division equations,

$$14 = 56 \times 1 - 42 \times 1 \tag{1}$$

$$42 = 322 \times 1 - 56 \times 5 \tag{2}$$

$$56 = 378 \times 1 - 322 \times 1. \tag{3}$$

Substituting (2) into (1), etc., gives

$$\begin{aligned} 14 &= 56 \times 1 - (322 \times 1 - 56 \times 5) \times 1 \\ &= 56 \times 6 - 322 \times 1 \\ &= (378 \times 1 - 322 \times 1) \times 6 - 322 \times 1 \\ &= 378 \times 6 - 322 \times 7. \end{aligned}$$

(You should check the result.) Multiplying the above equation by 2 gives

$$28 = 378 \times 12 - 322 \times 14. \quad (4)$$

So $378m + 322n = 28$ where $m = 12$ and $n = -14$.

4. (4 marks)

- (a) Find a pair of integers p and q , different from the pair m and n found in problem 3, such that $378p + 322q = 28$.

Note that $378(-322) + 322(378) = 0$. Adding that to equation (4) gives $378(12 - 322) + 322(-14 + 378) = 28$, i.e., $378(-310) + 322(364) = 28$, so one possible pair of p and q is $p = -310$ and $q = 364$.

- (b) Find a third pair of integers r and s , different from the pair m and n found in problem 3 and different from the pair p and q found in problem 4a, such that $378r + 322s = 28$.

Note that $378(322) + 322(-378) = 0$. Adding that to equation (4) gives $378(12 + 322) + 322(-14 - 378) = 28$, i.e., $378(334) + 322(-392) = 28$, so one possible pair of r and s is $r = 334$ and $s = -392$.

Question: How could you generate an infinite set of solutions to the equation $378m + 322n = 28$?

5. (3 marks) Prove that the number 391 is composite. (You can use a calculator if you wish.)

The square root of 391 is $19.77\dots$, so we need to try to divide 391 by primes from 2 to 19. When 391 is divided by 2 the remainder is $1 \neq 0$; when 391 is divided by 3 the remainder is $1 \neq 0$, etc., up to 17: when 391 is divided by 17 the remainder is 0 and the quotient is 23. So we have:

Theorem: 391 is composite. Proof: $391 = 17 \times 23$ where 17 and 23 are both greater than 1.

6. (5 marks) Find the prime factorization of 766360.

Here is a possible factorization tree:

$$\begin{array}{ccccccc}
 & & & & & & 766360 \\
 & & & & & / & \backslash \\
 & & & & & 10 & 38318 \\
 & & & & / & \backslash & | & \backslash \\
 & & & & 2 & 5 & 4 & 19159 \\
 & & & & & & / & \backslash & | & \backslash \\
 & & & & & & 2 & 2 & 7 & 2737 \\
 & & & & & & & & & / & \backslash \\
 & & & & & & & & & 7 & 391 \\
 & & & & & & & & & & / & \backslash \\
 & & & & & & & & & & 17 & 23
 \end{array}$$

Note I used the result of the previous problem! So the prime factorization of 766360 is $766360 = 2^3 \times 5 \times 7^2 \times 17 \times 23$.

7. (5 marks) Given any two integers a and b , not both 0, let $d = \gcd(a, b)$. Prove that the linear combination $ma + nb$ is a multiple of d for any integers m and n .

Since d is a divisor of a we can write $a = rd$ for some integer m . Since d is a divisor of b we can write $b = sd$ for some integer s . Then $ma + nb = m(rd) + n(sd) = (mr)d + (ns)d = (mr + ns)d$ where $mr + ns$ is an integer. Therefore $ma + nb$ is a multiple of d .

8. (8 marks) (Division with 'least non-positive' remainder.) Given integers a and b , $b > 0$, prove that there are unique numbers q and r such that $a = bq + r$ with $-b < r \leq 0$. (For example, dividing 20 by 3 in this way gives $20 = 3 \times 7 - 1$ instead of $20 = 3 \times 6 + 2$.)

Existence: The usual division algorithm guarantees the existence of integers q' and r' such that $a = bq' + r'$ such that $0 \leq r' < b$. If $r' = 0$ then let $q = q'$ and $r = r' = 0$, and you have shown the existence of q and r satisfying the given conditions. (Check!) On the other hand, if $r' > 0$, let $r = r' - b$ and $q = q' + 1$. Then $bq + r = b(q' + 1) + (r' - b) = bq' + b - b + r' = bq' + r' = a$ and $0 < r' < b$ implies $0 - b < r' - b < b - b$ implies $-b < r < 0$, so again, we have found q and r satisfying the given conditions. In all cases we have shown the existence of q and r satisfying the given conditions.

Uniqueness: Suppose there are two pairs of integers q_1, r_1 and q_2, r_2 satisfying the given conditions, i.e., $a = bq_1 + r_1 = bq_2 + r_2$ where $-b < r_1 \leq 0$ and $-b < r_2 \leq 0$. Then $b(q_1 - q_2) = r_2 - r_1$, and $-b < r_2 \leq 0$ and $0 \leq -r_1 < b$ which implies $0 - b < r_2 - r_1 < 0 + b$, i.e., $-b < r_2 - r_1 < b$. Summarizing, $r_2 - r_1$ is a multiple of b which lies between $-b$ and b , and is not equal to $-b$ nor to b . The only number satisfying those conditions is 0, so we must have $r_2 - r_1 = 0$ and $b(q_1 - q_2) = 0$, which imply $r_1 = r_2$ and (dividing through by b , which is possible since $b \neq 0$), $q_1 = q_2$.

9. (5 marks) Prove that if a, b, c are any three integers satisfying $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Here are three possible solutions.

(a) By the Euclidean algorithm, we can write

$$am + bn = 1 \tag{5}$$

$$ap + cq = 1 \tag{6}$$

for some integers m, n, p , and q . Multiplying equation (6) by b ,

$$am + bn = 1$$

$$apb + cqb = b$$

and substituting the second equation above into the first,

$$am + (apb + cqb)n = 1.$$

Rearranging,

$$a(m + pb) + bc(qn) = 1,$$

i.e., $ar + bcs = 1$ for some integers r and s . However, by the previous problem, $ar + bcs = 1$ is a multiple of $\gcd(a, bc)$, i.e., $\gcd(a, bc)$ divides 1. But the only divisors of 1 are 1 and -1 , so $\gcd(a, bc) = 1$.

(b) Alternatively, suppose p is a prime that divides $d = \gcd(a, bc)$. Then p divides a (because $a = dm$ and $d = pn$ so $a = pnm$) and p divides bc (similar reason). However, by Theorem 8.6.1 of the textbook, p divides bc implies that p divides b or p divides c . In the former case, p divides both a and b so p divides $\gcd(a, b)$, which is impossible because no prime p divides 1. In the latter case, p divides both a and c so p divides $\gcd(a, c)$, which is again impossible. All cases are impossible, which means that our original assumption that there is a prime which divides $\gcd(a, bc)$ must be wrong. There is no such prime, and the only positive integer which is divisible by no prime is 1, so we must have $\gcd(a, bc) = 1$.

(c) Courtesy of some students---I hadn't thought of this. Multiply equations (5) and (6) together to obtain

$$amap + amcq + bmap + bncq = 1.$$

Factoring,

$$a(map + mcq + bnp) + bc(nq) = 1.$$

i.e., $ar + bcs = 1$ for some integers r and s . As in 9a, $\gcd(a, bc)$ must then divide 1, which shows that it is 1.

10. (5 marks) The first few Fibonacci numbers are $f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, f_8 = 21$, and so on, where $f_{n+2} = f_{n+1} + f_n$ for $n \geq 1$. Show that any positive integer can be written as a sum of distinct Fibonacci numbers. (For example, we have $6 = 3 + 2 + 1$, but we can't write $6 = 3 + 3$ because 3 appears twice; $6 = 2 + 2 + 2$ and $6 = 1 + 1 + 1 + 1 + 1 + 1$ are also not allowed.)

Let's begin by exploring this situation. The first four paragraphs of this answer aren't required, but I have written them so that you may better understand the situation. One way to approach this question is to look at the similar case of the base 2 representation of the positive integers. Recall that any number can be represented in base 2 form; for example, $37 = (100011)_2$, which can be interpreted as $37 = 2^5 + 2^1 + 2^0$. Base 2 representation tells us that any positive integer can be written as a sum of distinct powers of 2. One way to find the base 2 representation of a number is to take out the largest power of 2 that fits in the number, and repeating the process on the difference until nothing remains. For example, the largest power of 2 that fits in 35 is $32 = 2^5$; taking away 32 from 35 gives $35 - 32 = 3$. The largest power of 2 that fits in 3 is $2^1 = 2$. Taking 2 from 3 leaves 1. The largest power of 2 that fits in 1 is $2^0 = 1$. Taking 1 from 1 leaves 0 and we are done.

That procedure is always guaranteed to work because there is a power of 2 that is equal to 1, so we could always take out 1's to get our number down to 0. However, An important outcome of this process is that no power of 2 is used more than once, not even 2^0 . Let us look at a similar situation to see how that outcome may fail so we can get a better idea of why it succeeds in the case of powers of 2. What if we have powers of 3 instead. Let's start again with 35. The largest power of 3 that fits in 35 is $3^3 = 27$. Taking 27 from 35 leaves 8. The largest power of 3 that fits in 8 is $3^1 = 3$. Taking 3 from 8 leaves 5. The largest power of 3 that fits in 5 is again $3^1 = 3$. Taking 3 from 5 leaves 2. The largest power

of 3 that fits in 2 is $3^0 = 1$. Taking 1 from 2 leaves 1. The largest power of 3 that fits in 1 is again $3^0 = 1$. Taking 1 from 1 leaves 0 and we are done.

Summarizing, we have $35 = 3^3 + 3^1 + 3^1 + 3^0 + 3^0$. We have used some powers of 3 more than once, which makes sense because in base 3 notation, $35 = (1022)_3$. In fact, it is unavoidable to use some powers of 3 more than once in general. The procedure still allows us to represent any number as a sum of powers of 3, but in general not distinct powers of 3.

The key difference between the two situations (powers of 2 and powers of 3) is that in the former, taking out the largest power of two that fits reduces the number so much that the same power of 2 will not fit again, and we will have to use a smaller power of 2. Each power of 2 is double the previous, whereas each power of 3 is more than double the previous.

The same kind of discussion applies in the case of the Fibonacci numbers. Since the Fibonacci numbers are increasing, each Fibonacci number, being the sum of the two previous, is less than or equal to the double of the previous Fibonacci number. (Write out a few Fibonacci numbers and check that the assertion is true for the numbers you pick.) So, given any number, taking out the largest Fibonacci number that fits results in a difference which is small enough that the same Fibonacci number will no longer fit. Somewhat more formally, if the number m lies between two consecutive Fibonacci numbers then we can write $f_{n+1} > m \geq f_n$; then $f_{n+1} - f_n > m - f_n \geq f_n - f_n$ which implies $f_{n-1} > m - f_n \geq 0$, so the largest Fibonacci number that will fit into $m - f_n$ is f_{n-2} , etc. Since 1 is a Fibonacci number, we can always find a Fibonacci number that will fit. Since the differences are decreasing, the procedure must always terminate. The result is established.

Two additional problems: 1) Show that the representation of a number as a sum of distinct Fibonacci numbers is not unique (unlike the base 2 representation); and 2) use strong induction to formalize the proof that any integer can be written as a sum of distinct Fibonacci numbers.