Math 238: Solutions to Homework

Steven Miller (sjm1@williams.edu)

November 22, 2011

Abstract

Below are solutions / sketches of solutions to the homework problems from Math 238: Number Theory (Smith College, Fall 2011, Professor Steven J. Miller, sjm1@williams.edu). The course homepage is

`http://www.williams.edu/Mathematics/`
`sjmiller/public_html/238.`

Note to students: it's nice to include the statement of the problems, but I leave that up to you. **I am only skimming the solutions. I will occasionally add some comments or mention alternate solutions. If you find an error in these notes, let me know for extra credit.**

Contents

1 HW #1: Due Thursday, September 15, 2011

Problem: #37.1 (a) Find a pattern involving F_m, F_n, F_{mn}. (b) Prove pattern true. (c) If $\gcd(m, n) = 1$ find a stronger pattern. (e) Prove pattern from (c) true.

Solution: (a) Lots of ways to try this. One possibility is Binet's formula, but then you have to prove a tricky expression is an integer. Another possibility is to try to use induction, but on what? On n? On m? Another is to try and use the recurrence relation. This might be promising, as it is THE fundamental piece of info. Of course, the first part is trying to figure out the pattern. A little experimentation shows $F_m|F_{mn}$ and $F_n|F_{mn}$, but F_mF_n does not necessarily divide F_{mn}.

For (b), once you have the pattern, try the following:

$$\begin{aligned} F_v &= F_{v-1} + F_{v-2} \\ &= F_{v-2} + F_{v-3} + F_{v-2} \\ &= 2F_{v-2} + 1F_{v-3} \\ &= 2(F_{v-3} + F_{v-4}) + F_{v-3} \\ &= 3F_{v-3} + 2F_{v-4} \\ &= 3(F_{v-4} + F_{v-5}) + 2F_{v-4} \\ &= 5F_{v-4} + 3F_{v-5}. \end{aligned}$$

As $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5$, ..., arguing as above we find we can write the above as

$$F_v = F_5F_{v-4} + F_4F_{v-5}.$$

Note the sum of the subscripts of the first product is $v + 1$, of the second is $v - 1$. In general, you can show

$$F_v = F_{k+1}F_{v-k} + F_kF_{v-k-1}.$$

Taking $v = mn$ and $k = m$ gives

$$F_{mn} = F_{m+1}F_{m(n-1)} + F_mF_{mn-n-1}.$$

We're almost done. The rest is an induction on n. We want to show, for any n, $F_m|F_{mn}$. Trivially true when $n = 1$. Assume true for $n - 1$ and must show true for n. Using the above relation, we have $F_{mn} = F_{m+1}F_{m(n-1)} + F_mF_{mn-n-1}$. By the inductive assumption, $F_m|F_{m(n-1)}$, and since $F_m|F_mF_{mn-n-1}$, we see that $F_m|F_{mn}$, completing the induction.

For (c), the stronger pattern is $F_mF_n|F_{mn}$ if $(m, n) = 1$ (this is how we write m, n relatively prime.

For (e) there are several approaches. A nice one is to note that the claim follows immediately if m, n relatively prime implies F_m and F_n are relatively prime. Why? If this is the case, then since $F_m | F_{mn}$ and $F_n | F_{mn}$, then $F_m F_n | F_{mn}$ as there are no common factors. We're just reduced to showing m, n relatively prime implies that F_m, F_n are relatively prime.

One way to see this is to use the fact that if two numbers are relatively prime, then by the Euclidean algorithm there are a, b such that $am + bn = 1$, with one of a, b positive and one negative. For definiteness, assume $a > 0$ and $b < 0$ so $am = cn + 1$ (with $c = -b$). Let's assume $d > 0$ divides F_m and F_n. Then from part (b) we know $d | F_{am} = F_{cn+1}$ (this is because $d | F_m$ and $F_m | F_{an}$); however, we also have $d | F_{cn}$ (this is because $d | F_n$ and $F_n | F_{cn}$). We now have F_{cn} and F_{cn+1} both divisible by d. As two adjacent Fibonacci numbers are divisible by d, so are *all* Fibonacci numbers from this point forward, due to the recurrence relation; moreover, running the recurrence relation *backwards* gives all previous Fibonacci numbers are divisible by d. As $F_1 = 1$, the only possibility is $d = 1$. Thus, F_m and F_n are relatively prime.

Problem: #37.3 (a) Make a list of Fibonacci numbers that are prime. (b) conjecture: if F_n is prime then what? (c) Does the conjecture work in reverse: if n is what then F_n is prime? (d) Prove conjecture in (b) is correct.

Solution: (a) $F_3, F_4, F_5, F_7, F_{11}, F_{13}, F_{17}, F_{23}, \ldots$.

(b) If F_n is prime then n is prime.

(c) Conjecture fails the other way: $F_{19} = 37 \cdot 113$.

(d) Assume the conjecture fails, and there is an F_n that is prime but $n = ab$ is composite. Then $F_a | F_n$ and $F_b | F_n$. Assume $a, b > 2$, then $F_a, F_b \geq 2$ and hence $1 < F_a, F_b < F_n$. In this case, we've just found a non-trivial factor of F_n and it cannot be prime. The only possibility left is if $a = b = 2$, in which case since $F_2 = 1$ neither F_a nor F_b is a non-trivial factor. Thus F_4 might be prime (it is, as it equals 3).

Problem: #37.5 (a) Find the first five terms of $A_n = 3A_{n-1} + 10A_{n-2}$ given $A_1 = 1, A_2 = 3$.

Solution: (a) 1, 3, 19, 87, 451, 2223, 11179. You should know how to write Mathematica code or excel code to do something like this. Mathematica would be

```
temp = {1, 3};
For[n = 1, n <= 5, n++,
  temp = AppendTo[temp, 10 temp[[n]] + 3 temp[[n + 1]]]];
```

```
Print[temp]
```

If you want to find the analogue of Binet's formula, you guess $A_n = r^n$, which leads to the equation $r^2 - 3r - 10r = 0$, which is $(r-5)(r+2) = 0$, so the roots are $5, -2$, and $A_n = c_1 5^n + c_2(-2)^n$. To have $A_1 = 1$, $A_2 = 3$ need to do some algebra to find c_1, c_2.

Problem: #37.9. The pattern has to repeat modulo m by the Pigeon hole principle. Imagine we get two 0s (modulo m) next to each other. Then using $F_{n+1} = F_n + F_{n-1}$, we see all future terms are 0 mod m, as are all previous. This contradicts $F_1 = 1$, so we cannot have two 0s next to each other modulo m.

Solution: As there are only finitely many patterns for pairs of numbers modulo m (there are at most m^2 patterns), at some point we must repeat. In other words, there are two consecutive pairs of Fibonacci numbers with the same values modulo m. By the recurrence relation, this gives us a cycle that repeats forwards and backwards. As we have $F_1 = 1$, $F_2 = 1$, the cycle must have 1, 1 in it, and thus going forward must have 1, 1 in it.

2 Second HW Assignment: Due Tuesday, September 20

Problem: #36.3. What is $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$?

Solution: Computing the answer for a few choices of n, we're led to believe it equals 2^n. Recalling that the binomial coefficients show up in Pascal's triangle, we're led to the Binomial Theorem, which states

$$(x+y)^n \ = \ \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

If we take $x = y = 1$, then we get

$$(1+1)^n \ = \ \sum_{k=0}^{n} \binom{n}{k},$$

proving the sum of the binomial coefficients is 2^n. Similarly, one can show the alternating sums has a very nice value too.

Problem: #36.6a. If p is prime then $\binom{p}{k}$ is divisible by p if $1 \le k \le p-1$. Find a k and an n such that $1 \le k \le n-1$ but $\binom{n}{k}$ is not divisible by n.

Solution: A brief search already turns one up with $n = 4$ and $k = 2$. There are three when $n = 6$ (corresponding to $k = 2, 3$ or 4). Here is some Mathematica code to find all exceptions for n up to 10.

```
For[n = 2, n <= 10, n++,
  For[k = 1, k <= n - 1, k++,
   If[Mod[Binomial[n, k], n] != 0,
     Print["(n,k) = (", n, ",", k, ") and (n choose k) = ",
      Binomial[n, k], "."]];
   ]];
```

Problem: Prove by direct computation that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Solution: Using $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, with $m! = m(m-1)\cdots 2\cdot 1$, we have

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= \frac{n!}{(k-1)!(n-k)!}\left[\frac{1}{k} + \frac{1}{n-k+1}\right] \\
&= \frac{n!}{(k-1)!(n-k)!}\left[\frac{n-k+1+k}{k(n-k+1)}\right] \\
&= \frac{n!}{(k-1)!(n-k)!}\frac{n+1}{k(n-k+1)} \\
&= \frac{(n+1)!}{k!(n-k+1)!} \;=\; \binom{n+1}{k}.
\end{aligned}$$

Problem: #41.9ab Let $L_1 = 1$, $L_2 = 3$ and $L_n = L_{n-1} + L_{n-2}$. (a) Find the first 10 terms. (b) Find a simple formula for the generating function.

Solution: (a) Working backwards (it will be needed later), we see $L_0 = 2$, and find the first few terms are 1, 3, 4, 7, 11, 18, 29, 47, 76, 123. Here's the Mathematica code to generate.

```
lucas = {1, 3};
For[n = 3, n <= 10, n++,
  lucas = AppendTo[lucas, lucas[[n - 1]] + lucas[[n - 2]]]];
Print[lucas]
```

For (b), the argument is very similar to class, except now the initial term is 2 instead of 0. Let $L(x) = \sum_{n=0}^{\infty} L_n x^n$. Then

$$\begin{aligned}
L_n(x) &= 2 + 1x + \sum_{n=2}^{\infty} L_n x^n \\
&= 2 + x + \sum_{n=2}^{\infty} (L_{n-1} + L_{n-2}) x^n \\
&= 2 + x + x\sum_{m=1}^{\infty} L_m x^m + x^2 \sum_{m=0}^{\infty} L_m x^m \\
&= 2 + x + x(L(x) - 2) + x^2 L(x) \\
(1 - x - x^2)L(x) &= 2 - x \\
L(x) &= \frac{2-x}{1-x-x^2}.
\end{aligned}$$

3 HW #3: Due Tuesday, September 27

Problem: #1.1: **EXTRA CREDIT:** Find the 3rd and 4th triangular numbers that are also square, and if possible the fifth. Can you find an efficient way to search? Do you think there are infinitely many?

Solution: Here is some code:

```
For[n = 1, n <= 10000, n++,
 If[IntegerQ[Sqrt[n (n + 1)/2]] == True,
  Print["n = ", n, " and T_n = ", n (n + 1)/2, " and square-root is ",
    Sqrt[n (n + 1)/2], "."]]]
```

It finds $T_1 = 1$, $T_8 = 36$, $T_{49} = 1225 = 35^2$, $T_{288} = 41616 = 204^2$, $T_{1681} = 1413721 = 1189^2$, and $T_{9800} = 48024900 = 6930^2$.

To find these efficiently, we know n and $n+1$ are relatively prime. Thus each is either a square or after division by 2 is a square. We can increase the search by breaking into the case n is even or odd. If n is odd then it must be a square, while if n is even then $n/2$ is a square. This *greatly* cuts down on the number of n to check. As the pattern seems to continue, I would guess there are infinitely many. One can try to solve $T_n = m^2$, use the quadratic formula....

Problem: #1.2. Find a pattern and prove it for the sum of the first n odd integers.

Solution: The sum of the first n odd numbers is n^2. Arrange them as a square. Start with a 1×1 square with just one dot. Then add the next odd number, 3, which gives a 2×2 square. Adding the next odd prime, 5, gives a 3×3 square.... Can also use induction. Base step is true. Inductive step: assume $1 + 3 + \cdots + (2n-1) = n^2$. Then

$$1 + 3 + \cdots + (2n-1) + (2n+1) \ = \ n^2 + (2n+1) = (n+1)^2,$$

as desired.

Problem: #1.3. Can there be three consecutive odd primes other than 3, 5, 7?

Solution: No. At least one of the three numbers must be divisible by 3, and hence composite as all numbers exceed 3 (we are looking for a triple other than the 3, 5, 7 one). To see this, there are three possibilities for our first number: it has remainder 0, 1 or 2 upon dividing by 3. If 0, then we've already shown one of the three consecutive odd numbers is composite. If the remainder is 1, then the second number in our sequence has remainder 0 when dividing by 3, while if the remainder of our initial number is 2 then the remainder of the last of our triples is 0 upon dividing by 3. Again we see the power of modular arithmetic.

Problem: #1.4. Say things about whether or not there are infinitely many primes of the form $N^2 - a$ for various a.

Solution: (a) Clearly not infinitely many of the form $N^2 - 1$ as it factors as $(N-1)(N+1)$; for $N > 4$ clearly our number $N^2 - 1$ is composite. For (b), no obvious obstructions appear and seems reasonable to have infinitely many primes. A lot show up....

```
For[n = 2, n <= 100, n++,
 If[PrimeQ[n^2 - 2] == True, Print[n, ", ", n^2 - 2]]]
```

(c) Similarly no obvious obstructions for $N^2 - 3$ and expect infinitely many, but $N^2 = 4 = (N-2)(N+2)$ and thus not infinitely many. (d) If a is not a square, seems likely that there are infinitely many primes of the form $N^2 - a$.

Problem: #2.1a. Show if $a^2 + b^2 = c^2$ is a primitive Pythagorean triple than either $3|a$ or $3|b$.

Solution: Note that $x^2 \equiv 0 \bmod 3$ if $x \equiv 0 \bmod 3$, and $x^2 \equiv 1 \bmod 3$ if x is either 1 or 2 modulo 3. Thus the sum of two squares modulo 3 is either $0 + 0 \equiv 0 \bmod 3$, $1 + 0 \equiv 1 \bmod 3$, or $1 + 1 \equiv 2 \bmod 3$. The last possibility cannot happen if we want the sum of the two squares to be a square, and thus either one or both of a and b must be divisible by 3.

Problem: #2.5a. Find a Pythagorean triple with $b = 4T_5$.

Solution: We have $T_5 = \frac{5 \cdot 6}{2} = 15$, thus from Theorem 2.1, page 17 we need $b = 60 = \frac{s^2 - t^2}{2}$, with $s > t \geq 1$ odd, relatively prime integers. First thought is need $s^2 - t^2 = 120$, so look at $120 + t^2$ for various choices of t. We find $t = 1, s = 11$ works, as does $t = 7, s = 13$ among others. Here is some code.

```
For[t = 1, t <= 100, t++,
 If[IntegerQ[Sqrt[120 + t^2]] == True,
  Print[t, " ", Sqrt[120 + t^2]]]]
```

Problem: If $ax^2 + bx + c$ has integer coefficients and one of the roots is rational then prove the other root is rational.

Solution: We have $a(x^2 + \frac{b}{a}x + \frac{c}{a}) = a(x - r_1)(x - r_2) = a(x^2 - (r_1 + r_2)x + r_1 r_2)$. Therefore $r_1 + r_2 = b/a$ and $r_1 r_2 = c/a$. As a, b are integers and assuming r_1 is rational, then $r_2 = \frac{b}{a} - r_1$ is rational, as the rational numbers are closed under division and subtraction.

4 HW #4: Due October 4

Problem: #3.2. (a) Using lines through $(1, 1)$, find all rational solutions to $x^2 + y^2 = 2$. (b) What goes wrong if we have $x^2 + y^2 = 3$.

Solution: (a) Equation of the line is $y - 1 = m(x - 1)$ for m some rational number (note that $(1, 1)$ is on this line). Solving gives $y = m(x - 1) + 1$, so $x^2 + (m(x - 1) + 1)^2 = 2$. Expanding gives $1 - 2m + m^2 + 2mx - 2m^2x + x^2 + m^2x^2 - 2$. We know $x - 1$ is a factor. Doing long division, we find the other factor is $(1 + 2m - m^2 + x + m^2x)$ (you could also get this with patience and the quadratic formula). This gives the other point on the line, with slope m, has coordinates $x = (-1 - 2m + m^2)/(1 + m^2)$ and thus $y = -(-1 + 2m + m^2)/(1 + m^2)$.

For (b), the problem is we cannot find a rational point on the circle! We need such a point to find others, but unable to find even one makes us realize how hard these problems can be.

Problem: #3.3. Find all rational points on the hyperbola $x^2 - y^2 = 1$.

Solution: Similar to earlier problems. This time there are clearly points, such as $(-1, 0)$. Now the sloper-intercept form of the line with slope m going through this point is $y = m(x + 1)$. Substituting into the hyperbola gives $x^2 - m^2(x + 1)^2 = 1$. We factor again, either knowing that $x + 1$ has to be a root, or using the quadratic formula. We find the other factor is $(1 + m^2 - x + m^2x)$ and the other root is $x = \frac{m^2-1}{m^2+1}$, $y = \frac{2}{m^2-1}$.

Problem: #5.1a Find $\gcd(12345, 67890)$.

Solution: Note $\lfloor 67890/12345 \rfloor = 5$, so first step is $67890 - 5 \cdot 12345 = 6165$. So $\gcd(12345, 67890)$ $= \gcd(6165, 12345)$. Now $\lfloor 12345/6165 \rfloor = 2$, so next step is $12345 - 2 \cdot 6165 = 15$, and thus $\gcd(12345, 67890) = \gcd(15, 6165)$. As 6165/15 = 411, we see 15 divides 6165. Thus $\gcd(15, 6165) =$ 15, and hence the original gcd is 15. While Mathematica has its own greatest common divisor function built in, it's easy (and somewhat fun!) to write one:

```
gcdfunction[xx_, yy_] := Module[{},
   x = Min[xx, yy]; y = Max[xx, yy];
   While[x > 0,
    {
     While[y >=  x, y = y - x];
     r = y; (* store current y value in r *)
     y = x; (* make current x value new y *)
     x = r; (* make the old y value the new x value *)
     }];
   Print[y]; (* this is the gcd *)
   ];
```

Problem: #5.3. Show that every two iterations of the Euclidean algorithm decrease the remainder by at least 1/2.

Solution: See Chapter 1 of my book, Section 1.2.
`http://press.princeton.edu/chapters/s8220.pdf`. A better solution, suggested by the class, is to note $r_i > r_{i+1} > r_{i+2}$, $r_i = q_{i+1}r_{i+1} + r_{i+2}$, and since $q_{i+1} > 0$, $r_i > r_{i+1} + r_{i+2} \geq 2r_{i+2}$, as desired.

Problem: #5.4abce. (a) Find some least common multiples, (b) compute in terms of components and greatest common divisor, (c) give argument that the found relationship is correct, (e) consider $\gcd(m, n) = 18$ and $\text{lcm}(m, n) = 720$, does this uniquely determine m and n?

Solution: (a) $\text{lcm}(8, 12) = 24$, $\text{lcm}(20, 30) = 60$, $\text{lcm}(51, 68) = 204$, $\text{lcm}(23, 18) = 414$.

(b) We see in each case that $\text{lcm}(m, n) \gcd(m, n) = mn$.

(c) By fundamental theorem of arithmetic every integer can be written uniquely as a product of prime powers. Say p^k divides mn. If p only divides one of m, n then p^k doesn't divide the gcd but is the highest power of p dividing the lcm, and thus all is good. If p divides both m, n, say $p^i|m$ and $p^j|n$ (with $i+j = k$). Without loss of generality, assume $i < j$. Then the power of p dividing the gcd is i and the power of p dividing the lcm is j, and we get both sides are divisible by p^{i+j} (but no higher power of p).

(e) By (c), we know $\text{lcm}(m, n) \gcd(m, n) = mn$; by the givens of the problem, $\text{lcm}(m, n) \gcd(m, n) = 18 \cdot 720 = 12960 = 2^5 3^4 5$. So any grouping of the factors of 12960 into m and n is valid. For m, there are 6 choices as to the power of 2 (including having no power of 2), 5 choices for the power of 3, and 2 choices for the power of 5 (if we choose no powers at all, then m is just 1). Thus there are $6 \cdot 5 \cdot 2 = 60$ pairs. The are all numbers of the form $(m, n) = (2^a 3^b 5^c, 2^{5-a} 3^{4-b} 5^{1-c})$, with $0 \leq a \leq 5$, $0 \leq b \leq 4$ and $0 \leq c \leq 1$. We need to do a little more work, though. As the greatest common divisor is 18, no number can be lower than 18 and must be divisible by 18. Further, the least common multiple is 720, so neither number can be larger than 720. So let's pull $18 = 2 \cdot 3^2$ out from each. Thus $(m, n) = 18(2^a 5^c, 2^{3-a} 5^{1-c})$, with $0 \leq a \leq 3$ and $0 \leq c \leq 1$. Can't have $a = 3, c = 1$ or $a = 0, c = 0$ as then exceeds least common multiple. Possibilities are thus $18(1, 40), 18(5, 8), 18(2, 20), 18(4, 10)$; however, only the first two pairs are relatively prime (and thus the others have a larger greatest common divisor). Thus the answer is $18(1, 40) = (18, 720)$ and $18(5, 8) = (90, 144)$ (and of course $(720, 18)$ and $(144, 90)$). One could also write a compute code to investigate. Here's my Mathematica code, using that $xy = \gcd(x, y)\text{lcm}(x, y) = 12960$.

```
For[a = 0, a <= 5, a++,
  For[b = 0, b <= 4, b++,
   For[c = 0, c <= 1, c++,
    {
     x = 2^a 3^b 5^c;
     y = 12960/x;
     If[LCM[x, y] == 720 && GCD[x, y] == 18,
      Print["x = ", x, " and y = ", y, "."]];
     }]]];
```

5 HW #5: Due Tuesday, October 11

Problem: Page 4 of my book, #1.1.1. There are approximately 10^{80} elementary objects in the universe (photons, quarks, et cetera). Assume each such object is a powerful supercomputer capable of checking 10^{20} numbers a second. How many years would it take to check all numbers (or all primes) less than $\sqrt{10^{400}}$? What if each object in the universe was a universe in itself, with 10^{80} supercomputers: how many years would it take now?

Solution: The number of seconds in a year is $60 \cdot 60 \cdot 24 \cdot 365.25 \approx 3.15576 \cdot 10^7$. If t is the number of seconds needed, to check the 10^{200} numbers requires $10^{200}/(10^{80} \cdot 10^{20}) = 10^{100}$, or $3 \cdot 10^{92}$ years! Even if every subatomic particle was an entire universe, we'd still need about $3 \cdot 10^{12}$ years!

Problem: Page 9 of my book, #1.2.17: Give a non-constructive proof of the existence of $ax + by = \gcd(x, y)$.

Solution: Step 1: As the non-negative integers have a smallest element, we can look at all choices of a and b that lead to a positive value, and take a choice that gives the smallest positive value (note this set is non-empty – take $a = b = 1$). We let d be the smallest value attained, and let α, β be values where it is attained, so $d = \alpha x + \beta y$. It's very important that we are looking at integers and not rational numbers, as there is no smallest positive rational number. For each positive integer we can ask if it can be represented as a linear combination. We know at least one positive integer can, so this set is not empty. Now we just need to look and find the smallest, and fortunately the set *will* have a smallest element.

Step 2: Claim $\gcd(x, y)|d$. As d is a linear combination of x and y, anything that divides both x and y divides d, and the claim follows. Specifically, as α, β are integers, $d|x$ means $d|\alpha x$, and similarly $d|y$ implies $d|\beta y$. Thus d divides the sum, $\alpha x + \beta y$.

Step 3: Let $e = Ax + By$ for any A, B. Claim $d|e$. If not, write e as a multiple of d plus a non-zero remainder modulo d, say $r \in \{0, 1, \dots, d-1\}$. By subtracting, we find A', B' such that $r = A'x+B'y > 0$ and $r < d$. This contradicts the minimality of d, contradiction, so $d|e$.

Step 4: Taking $(A, B) = (1, 0)$ and $(0, 1)$ we see $d|x$ and $d|y$, and so d is the greatest common divisor of x and y. This shows us the power of taking special cases in a general formula.

Problem: Page 15 of my book: #1.3.9: Find rules for divisibility by 3, 9, 11 and 7.

Solution: As $10^n \equiv 1 \bmod 3$ (or modulo 9), we have $\sum_{n=0}^{N} a_n 10^n \equiv \sum_{n=0}^{N} a_n \bmod 3$ (or modulo 9), and thus a number is divisible by 3 (or 9) if and only if the sum of its digits is divisible by 3 (or 9). For 11, notice that $10^n \equiv 1 \bmod 11$ if n is even and $-1 \bmod 11$ if n is odd. Thus instead of a sum of the digits we have an alternating sum of digits, and our number is divisible by 11 if and only if the alternating sum is divisible by 11. For example, 451 is divisible by 11 (and 4-5+1 is 0 modulo 11), while 452 is not (here 4 - 5 + 2 is 1 modulo 1). For 7, the formula isn't clean; we just look at the different remainders of powers of 10 modulo 7 and get a weighted sum.

Problem: Page 15 of my book: #1.3.10 (don't do the last part): Given m_1, m_2 relatively prime and a_1, a_2 arbitrary integers, prove there is a unique $x \bmod m_1m_2$ such that $x \equiv a_i \bmod m_i$.

Solution: Here is some code to investigate the problem and find answers:

```
chineseremainder[m1_, m2_, a1_, a2_] :=
 If[GCD[m1, m2] > 1, (* checks to see if numbers relatively prime *)
  Print["Why did you give me two moduli that aren't relatively prime?"],
  For[x = 0, x <= m1 m2 - 1, x++, (* here if numbers relatively prime *)
   If[Mod[x - a1, m1] == 0 && Mod[x - a2, m2] == 0, Print[x]];
  ]; (* end of For statement *)
 ]  (* end of If statement *)
```

Your first thought when you see problems like this and are given phrases such as 'relatively prime' is the Euclidean algorithm, or more precisely the linear combination consequence. As m_1, m_2 are relatively prime there are integers α, β such that $\alpha m_1 + \beta m_2 = 1$. This means that $\alpha m_1 \equiv 1 \bmod m_2$ and $\beta m_2 \equiv 1 \bmod m_1$. Look at $a_2 \alpha m_1 + a_1 \beta m_2$. Modulo m_2, this is just a_2, while modulo m_1 it is a_1. Thus this number satisfies our requirements. The idea is to use the Euclidean algorithm and exploit it to get expressions that are equivalent to 1. If we had two different x that worked, if we subtracted these from each other we would get a non-zero number modulo $m_1 m_2$ that is equivalent to 0 modulo m_1 and m_2. As m_1 and m_2 are relatively prime, this cannot happen.

Problem: Look at all numbers of the form $3x + 5y$, where x and y are non-negative integers. What values occur as we vary x and y? Prove your conjecture.

Solution: Direct calculation gives us 3, 5, 6, 8, 9, 10, 11, 12, ... Once we have three numbers in a row, we have all integers from that point onward, as we can just keep adding copies of 3 and marching down.

Problem: Let x, y, and z range over the positive integers. Describe all numbers of the form $6x + 10y + 15z$. In general, if a, b and c are given and x, y and z range over all positive integers, what numbers are attainable as $ax + by + cz$?

Solution: Let's build some intuition by looking at attainable integers.

```
list = {6, 10, 15};
For[i = 0, i <= 5, i++,
  For[j = 0, j <= 5, j++,
   For[k = 0, k <= 5, k++,
    {
     x = 6 i + 10 j + 15 k;
     If[MemberQ[list, x] == False, list = AppendTo[list, x]];
     }]]];
list = Sort[list]
```

First, assume we could have zero for x, y, z and not have to take positive integers. This gives 6, 10, 12, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, ... Once we have 6 consecutive elements, we're done, and thus we see we get everything from 24 onward. All the requirement of positivity does is shift everything a bit. We now get 6, 10, 15, 31, 37, 41, 43, 46, 47, 49, 51, 52, 53, 55, 56, 57, 58, 59, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, ... We get everything from 61 onward, and notice that 61 is one more than twice the least common multiple.

If a, b, c have a common factor dividing all, then that factor divides all attainable numbers. Let's therefore assume a, b, c are relatively prime. We can prove that there is some integer such that we attain all integers from there onward. The reason is that it just suffices to get one element of each congruence class, and then we can get everything from that point onward. The problem is much easier if we don't require x, y, z to be positive. We first choose y', z' such that $10y' + 15z' = \gcd(10, 15) = 5$. As $\gcd(6, 5) = 1$, we can choose x and x' such that $6x + 5x' = 1$, or $6x + 10y + 15z = 1$, with $y = y'x'$ and $z = z'x'$. If we then multiply by k, we see we can get any positive integer. This idea generalizes. Clearly if $\gcd(a, b, c) = d$ then all numbers are multiples of d, and we can get any multiple. If $d = 1$ (as we are assuming as all are relatively prime), then we can find x', y', z' with $ax' + by' + cz' = 1$. By looking at this modulo a, we find positive integers y'', z'' with $by'' + cz'' \equiv 1 \bmod a$. Thus, by taking enough copies of this, we can get remainders of 1, 2, 3, . . . , a modulo a, and hence get all numbers from some point onward. As to what's the smallest point from which we get everything, that's more involved.

Problem: Gather data and make some conjectures (prove if possible): let x and y be relatively prime positive integers. Are there non-zero integers a and b such that $a^2x+b^2y=1$? What about $a^3x+b^3y=1$? Maybe the answer is yes for some x and y and no for others....

Solution: There are no solutions to $a^2x+b^2y=1$ if x,y are relatively prime positive integers. This is because a^2x and b^2y are each at least 1. It's much more interesting if we deal with cubes, as then if a and b are of opposite sign, we can have cancelation. Here's a quick Mathematica program to investigate:

```
x = 3; y = 10; m = 2000;
count = 0;
For[a =  1, a <= m, a++,
 For[b = 1, b <= m, b++,
   {
    If[a^3 x - b^3 y == 1 ||  -a^3 x + b y^3 == 1 ,
      {
       count = count + 1;
      If[count == 1, Print["a = ", a, " and b = ", b]];
      }];
    }];
 ]
```

This finds the solution $a=3$ and $b=2$. If now we take $x=5, y=7$ and increase m up to 4,000, no solutions are returned. So, maybe there are choices of x and y without solutions? In problems like this, congruences are often useful. If $p \equiv 1 \bmod 3$, then $a \mapsto a^3 \bmod p$ is not an isomorphism; we get $(p-1)/3+1$ distinct elements modulo p.

Here's a program to investigate a specific choice of x and y (same as above) and using congruences to attack it. The trick is to note that if we cube the numbers and look modulo p, if $p \equiv 1 \bmod 3$ then the image isn't all congruence classes, but basically just one-third. If we choose our prime to be one of our numbers, then $a^3x+b^3y \equiv a^3x \bmod y$, and thus by the Pidgeon-hole principle we can find an x such that this fails! In other words, so long as $y \equiv 1 \bmod 3$ is prime, there'll always be an x such that there are no solutions! The following code proves there are no solutions for $x=5, y=7$ (I included the power feature so we could look at prime powers and not just primes for the modular arguments, while the degree feature is to investigate more than just cubics).

```
number = 7;
power = 1;
x = 5;
y = 7;
deg = 3;
list = {0};
For[n = 1, n <= number - 1, n++,
  {
   tempnum = Mod[n^deg, number^power];
   If[MemberQ[list, tempnum] == False,
    list = AppendTo[list, tempnum]];
   }];
list = Sort[list]
For[a = 1, a <= Length[list], a++,
  For[b = 1, b <= Length[list], b++,
   If[Mod[Abs[list[[a]] x - list[[b]] y], number^power] == 1,
     Print[list[[a]], " " , list[[b]]]]];
   ]];
```

Here's another way to look at it. Let's take x and y to be two cubes, say $x = \widetilde{x}^3$ and $y = \widetilde{y}^3$. Then we're trying to find cubes a and b so that $a^3x + b^3y = 1$, or $(a\widetilde{x})^3 + (b\widetilde{y})^3 = 1$. There's a beautiful theorem that completely resolves this. It's known as either Mihailescu's theorem (as he proved it) or Catalan's conjecture, and states that the only adjacent non-trivial integer powers (non-trivial means the exponents of each exceed 2) are $(0, 1)$, $(-1, 0)$ and $(8, 9)$. In other words, if we want to solve $x^m - y^n = 1$ with x, y integers and $n, m \geq 2$ positive integers, these are the only pairs that work. Letting $\widetilde{b} = -b$, our equation $a^3x + b^3y = 1$ becomes $(a\widetilde{x})^3 - (\widetilde{b}\widetilde{y})^3 = 1$. By Mihailescu's theorem, there are no two adjacent cubes, and thus there are no solutions!

6 HW #6: Due Tuesday, October 25

Problem: Chapter 12, Page 83: #12.2a. Show infinitely many primes congruent to 5 modulo 6.

Solution: Modify Euclid's proof. Assume not, so $p_1, \dots, p_N$ is a complete list. We have $p_1 = 5, p_2 = 11, p_3 = 17, p_4 = 23, p_5 = 29, p_6 = 41$ and so on (pretty amazing how many in a row we had). Then $x_N = 6p_2 \cdots p_N + 5$ is congruent to 5 modulo 6; note we are NOT including the prime $p_1 = 5$. If x_N is prime, we have found a new prime congruent to 5 modulo 6 that is not on our list. Assume then that x_N is composite; the proof is completed by showing it is divisible by a prime congruent to 5 modulo 6 that is not in our list. Clearly x_n is not divisible by 2 or 3 or 5. All primes may be written as either 2, 3, or of the form $6n+1$ or $6m+5$ for some n or m. As 2, 3 and 5 do not divide x_N, all its prime factors are of the form $6n+1$ or $6m+5$. If all of the primes are congruent to 1 modulo 6, so too is their product, which contradicts x_N is 5 modulo 6. Thus x_N is divisible by a prime congruent to 5 modulo 6 not on our list, completing the proof.

Problem: Chapter 12, Page 83: #12.5abc.

Solution: (a) Highest power of 2 dividing 1! is 0, 2! and 3! is 1, 4! and 5! is 3, 6! and 7! is 4, 8! and 9! is 7, and 10! is 8. (b) What is the highest power of 2 dividing $n!$? Let $\lfloor x \rfloor$ represent the floor function, the largest integer at most x. The highest power of 2 is $\sum_{k=1}^{\log_2 n} \lfloor n/2^k \rfloor$. To see this, keep track of how many integers are divisible by 2, then by 4, then by 8, and so on. For example, a number divisible by 8 will be counted three times. If $n = 100$ we get 97, if $n = 1000$ we get 994. The Mathematica code is

```
Sum[Floor[n/2^k], {k, 1, Log[2, n]}]
```

(c) We already gave the proof; we count each number once if divisible by 2, again if divisible by 4, again if divisible by 8, ...

Problem: Chapter 13, Page 89:#13.1b. Explain why 'most numbers are not squares' makes sense.

Solution: If $S(x)$ is the number of squares at most x, we have $\sqrt{x} - 1 \le S(x) \le \sqrt{x}$. Thus the percentage of numbers that are square and at most x is in $[x^{-1/2} - x^{-1}, x^{-1/2}]$. As $x \to \infty$, the percentage tends to zero. Note $S(x) \approx \sqrt{x}$ (and the error is at most 1).

Problem: Chapter 13, Page 89: #13.3. Show that $n!+2, n!+3, \dots, n!+n$ are all composite. Conclude there are arbitrarily large gaps.

Solution: Note 2 divides $n! + 2$, 3 divides $n! + 3$, and so on up till n divides $n! + n$. Thus these $n - 1$ numbers are composite. By taking n sufficiently large, we can have as big of an interval as desired without prime numbers. The problem with this method is the bound sucks (for example, this method tells us we'll have a gap of size at least 100 by $100! + 100 \approx 9.33 \cdot 10^{157}$; however, the first gap of size at least 100 is between the primes 370,261 and 370,373. A better estimate is to use primorials, $n!_p$, where $7!_p = 7 \cdot 5 \cdot 3 \cdot 2$ and $11!_p = 11 \cdot 7!_p$.

Problem: Chapter 13, Page 89: #13.5. Justify the following.

Solution: (a) By the Prime Number Theorem, there are about $x/\log x$ primes at most x, so the density of primes is about $(x/\log x)/x$ or $1/\log x$. Thus we have about a one in $\log x$ of choosing a number in $[1, x]$ and getting a prime. One issue with estimates like this is that the density is very different near the extremes of the interval. Let's look at the interval $[x, 2x]$ which has approximately $\frac{2x}{\log 2x} - \frac{x}{\log x} \approx \frac{x}{\log x}$ primes. As the interval has length x, the density of primes here is about $1/\log x$. (b) Assuming independence (a big assumption), if each number at most x is prime with probability $1/\log x$, the probability two are prime would be $1/\log^2 x$. Okay, it's really $\frac{1}{\log x}\frac{1}{\log(x+2)}$, but for x large the error in replacing $\log(x+2)$ with $\log x$ is very small. Using Taylor series, we have

$$\log(x+2) \;=\; \log x + \log\left(1 + \frac{2}{x}\right) \;=\; \log x + \frac{2}{x} - \frac{2}{x^2} + \frac{8}{3x^3} - \cdots .$$

(c) Same as (b), except instead of two random integers it is two consecutive integers. Note that these problems completely ignore some obvious congruence issues (for example, if $n \equiv 1 \bmod 3$ then there is no way n and $n+2$ can both be prime). In fact, continuing this argument you'd be led to the absurdity that the probability n, $n+2$ and $n+4$ are all prime is about $1/\log^3 n$, which is clearly false. The point is to get a rough heuristic, and then incorporate the true, relevant facts.

Problem: Prove $\sum_{n=1}^{\infty} 1/n^2$ converges, and find its value to within 1/2011.

Solution: This converges by the integral test (it is a p-series with $p = 2$. It's a beautiful result that this equals $\pi^2/6$ (the exact value). If we sum the first N terms, the error is

$$\sum_{n=N+1}^{\infty} \frac{1}{n^2} \;\le\; \int_N^{\infty} \frac{dx}{x^2} \;=\; \frac{1}{N}.$$

Thus we're safe if we take $N = 2011$, which gives approximately 1.644436925. The Mathematica code and output is

```
1/2011.
SetAccuracy[Sum[1/n^2, {n, 1, 2011}], 10]
SetAccuracy[Pi^2/6, 10]

0.000497265

1.644436925

1.64493407
```

7 HW #7: Due Tuesday, November 8

Problem: Chapter 35, Page 282: #35.1a If N is not a perfect square, prove $\sqrt{N}$ is irrational.

Solution: We use the Fundamental Theorem of Arithmetic. We may write N as $p_1^{r_1} \cdots p_k^{r_k}$, where the primes are distinct and at least one power is odd (as otherwise N would be a perfect square). If $\sqrt{N}$ were rational, we could write it as $\sqrt{N} = p/q$, with p, q relatively prime. This would imply $N = p^2/q^2$, or $q^2 N = p^2$. Note the right hand side is a perfect square, but the left is not as N is not a perfect square (and a perfect square times a perfect square, such as q^2, is a perfect square). Contradiction. We could rephrase the argument and take a prime that divides N exactly an odd number of times. Even if it divides q, it would divide the left hand side an odd number of times. By the Fundamental Theorem of Arithmetic, it would have to divide p^2, and hence p, and thus divide the right hand side an even number of times, a contradiction.

Problem: Chapter 35, Page 282: #35.3. Find degree 3 polynomials with integer coefficients with various properties.

Solution: (a) Three distinct rational roots: $x(x-1)(x+1)$. (b) One rational root and two irrational roots: $x(x^2-2)$. (c) No rational roots: $x^3 - 2$. (d) Can a polynomial of degree 3 have two rational roots and one irrational root? Yes: $x^2(x+\sqrt{2})$. If, however, our polynomial is to have integer coefficients, the answer is no. Assume $ax^3 + bx^2 + cx + d = a(x-r_1)(x-r_2)(x-r_3)$. Note $b = -a(r_1 + r_2 + r_3)$. If the first two roots are rational, then (assuming $a \neq 0$, which is reasonable as we're assuming we have a degree 3 polynomial), $r_3 = (b + ar_1 + ar_2)/a$ and thus the third root is rational.

8 HW #10: Due Tuesday, November 15

Problem: Chapter 5 of my book. Exercise 4.24 (just do the first part, for p/q to be a root).

Solution: We have $f(x) = a_n x^n + \cdots + a_0$, and assume $f(p/q) = 0$ for relatively prime p and q. Then after some straightforward algebra we find $(a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n)/q^n = 0$, or $a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$. As p divides every term but $a_0 q^n$, and $p|0$, we must have $p|a_0 q^n$. As p cannot divide q (they are relatively prime), $p|a_0$. Similarly, we see q divides all the terms but the first, $a_n p^n$. As q cannot divide p^n, $q|a_n$. Thus there are only finitely many candidates to check for a rational root!

9 HW #11: Due Tuesday, November 22

Problem: Chapter 19: #19.3abc

Solution: We need to factorize 1105, 1235, and 2821. We get $1105 = 5 \cdot 13 \cdot 17$, $1235 = 5 \cdot 134 \cdot 19$, and $2821 = 7 \cdot 13 \cdot 31$ (to see this, we can use our tricks for divisibility by 2, 3, 5, 9, and 11, and then do the rest by brute force). We see all are odd, none are divisible by a prime square, and thus half of Korselt's criteria are met. We must show for each number that $p - 1 | n - 1$ for it to be a Carmichael number. Doing the algebra, we see 1105 and 2821 are Carmichael numbers, but 1235 is not (1234 is not divisible by 6).

Problem: #19.4a (as well as find one number that works).

Solution: By assumption, $n = (6k + 1)(12k + 1)(18k + 1)$ is the product of three distinct odd primes (or a unit if $k = 0$). Thus to see it is Carmichael we must show mk divides $n - 1$ for $m \in \{6, 12, 18\}$. We have $n - 1 = 36k + 396k^2 + 1296k^3$, which factors as $n - 1 = 36k(1 + 11k + 36k^2)$. Thus $6k, 12k, 18k$ all divide $n - 1$, and it is a Carmichael number.

Problem: State a result about Carmichael numbers that is not covered in Chapter 19 of the book, or the three papers mentioned above.

Solution: See `http://www.maths.lancs.ac.uk/~jameson/carfind.pdf`, page 2, Proposition 4: *Suppose that n is a Carmichael number and that p and q are prime factors of n. Then q is not congruent to 1 mod p.*