Intro to Number Theory: Solutions

Dr. David M. Goulet

November 14, 2007

Preliminaries

Base 10 Arithmetic

Problems

- What is $7777 + 1$ in base 8?

  Solution: In base 10, $7 + 1 = 8$, but in base 7, $7 + 1 = 10$. So $7777 + 1 = 7770 + 10 = 7700 + 100 = 7000 + 1000 = 10000$.

- In what base is 21^2 equal to 225_{10} ?

  Solution: call the base b. Then in base 10, $(2 * b + 1)^2 = 225$. So $2b + 1 = 15$. Thus $b = 7$.

- You ask your cyborg friend what it would like to eat. It replies "48,879". Knowing that your cyborg friend thinks in hexidecimal but speaks in decimal, what should you feed it?

  Solution: It's first useful to compute some powers of 16; $16^2 = 256$, $16^3 = 4096$, and $16^4 = 69632$. Notice that this last power of 16 is larger than the given number, so we'll only need 4 hexidecimal digits. The largest multiple of 4096 that can be subtracted from 48869 is 11, which in hexidecimal is B. This leaves 3823. The largest multiple of 256 which can be subtracted from this is 14, or E, which leaves 239. Continuing this, we find that out cyborg friend asked for "BEEF".

Fundamental Theorem of Arithmetic

Problems

- Factor 120 uniquely into primes. Solution $120 = 2 * 60 = 2^2 * 30 = 2^3 * 15 = 2^3 * 3 * 5$.

- Three inegers (x, y, z) satisfy $34x + 51y = 6z$. If y and z are primes, what are these numbers?

  Solution: Writing $17(2x + 3y) = 6z$ shows that z is divisible by 17. Because z is a prime, we must have $z = 17$. We can now divide the whole expression by 17 to get $2x+3y = 6$. Writing this as $3y = 2(3-x)$ shows that y is divisible by 2. Because y is a prime, $y = 2$. Finally $x = 0$.

- Prove that $\sqrt{p}$ is an irrational number for any prime p.

  Solution: Suppose that $\sqrt{p}$ is a rational number. Then there exist two integers, n and m with no common divisor such that $\sqrt{p} = n/m$. This shows that $pm^2 = n^2$, so p must divide n^2. Just as the proof above for $\sqrt{2}$, this shows that p divides n which means that p^2 divides n^2. This shows that p divides m^2, which again shows that p divides m. This is a contradiction, because m and n have no common divisors. So $\sqrt{p}$ is not rational.

- Suppose that p is the largest prime number. Is $p! + 1$ divisible by any primes $\leq p$? Is this a contradiction?

  Solution: The number $p!$ is divisible by all primes $\leq p$. Can you see why? However, 1 isn't divisible by any of these primes. So $p! + 1$ isn't divisible by any primes $\leq p$. But the fundamental theorem of arithmetic tells us that every number is either prime or divisible by primes. So, because $p! + 1$ isn't divisible by any primes $\leq p$, it must be divisible by some prime $> p$ or it must itself be a prime. This is a contradiction, because p was assumed to be the largest prime. We conclude that there is no largest prime.

Divisibility Tests

Divisibility by Powers of 2

Problems

- Is $1,234,567,890$ divisible by 2?

  Solution: The last digit is 0, which is divisible by 2. So $1,234,567,890$ is divisible by 2.

- Is $121^{13} - 101^4$ divisible by 2?

  Solution: Any number ending in 1, when raised to any power, still ends in 1. Can you see why? So both 121^{13} and 101^4 end in 1. This means that their difference ends in 0, which is divisible by 2. So $121^{13} - 101^4$ is divisible by 2.

- Prove that $1782^{12} + 1841^{12} \neq 1922^{12}$. Do you know why your calculator is wrong?

  Solution: 1782^2 and 1922^2 are each divisible by 2, while 1841^2 is not. Can you see why? So the equation can't be true. Your calculator is wrong because these numbers have over 40 digits and your calculator can't accurately keep track of them all when computing the additions, subtractions, and roots.

- How do you prove the 2^n case?

  Solution: Notice that 100 is divisible by 4, that 1000 is divisible by 8 and that in general 10^n is divisible by 2^n. So, we can write any k digit number as $m = d_k d_{k-1} \dots d_2 d_1 = 10^n (d_k \dots d_{n+1}) + d_n d_{n-1} \dots d_2 d_1$. So m is divisible by 2^n if and only if $d_n \dots d_1$ is.

Divisibility by 3 and 9

Problems

- Does the above proof also work for the case of divisibility by 9?

  Solution: Yes. As you can see, all of the terms that were described as being divisible by 3 are actually divisible by 9 as well.

- Is $1,234,567,890$ divisible by 3?

  Solution $1+2+3+4+5+6+7+8+9+0 = 45$ and 45 is divisible by 3 because $4+5=9$ and 9 is divisible by 3.

- Is $326^2 - 325^2$ divisible by 3?

  Solution: In algebra we learn about factoring the difference of two squares, $x^2 - y^2 = (x-y)(x+y)$. Using this formula here gives $326^2 - 325^2 = (326-325)(326+325) = (1)(651) = 651$. This is divisible by 3 because $6+5+1 = 12$.

- Is $65,314,638,792$ divisible by 24?

  Solution: $6+5+3+1+4+6+3+8+7+9+2 = 54$ and 54 is divisible by 3 because $5+4=9$. So the number is divisible by 3. To check for divisibility by 8, we look at the last three digits, 792. This is divisible by 8 $(792/8 = 99)$. So the number is divisible by both 8 and 3. So it must be divisible by $8*3 = 24$.

Divisibility by Powers of 5

Problems

- Is $1,234,567,890$ divisible by 5?

  Solution: The last digit is 0 which is divisible by 5, so the number is divisible by 5.

- How many 3 digit numbers are divisible by 5?

  Solution: The only numbers divisible by 5 are numbers which end in 5 or 0. So we want to know how many numbers between 99 and 1000 end in a 5 or a 0. The first one is 100 and the last is 995, so there are $1 + (995-100)/5 = 180$ such numbers.

- Find a divisibility test for 125. Use your test to decide if $1,234,567,890,000$ is visible by 750.

  Solution: Notice that 100 is divisible by 25, that 1000 is divisible by 125 and that in general 10^n is divisible by 5^n. We write any k digit number as $m = d_k \dots d_1 = 10^n(d_k \dots d_{n+1}) + d_n \dots d_1$. So a number is divisible by 5^n if and only if it's last n digits form a number which is divisible by 5^n. Because $750 = 2 * 3 * 5^3$, we check for divisibility by 2, 3, and 5^3. The last digit is 0, so the number is divisible by 2. $1+2+3+4+5+6+7+8+9 = 45$ so the number is divisible by 3. The last three digits are 000 which is divisible by 125, so the number is divisible by 5^3. So, the number is divisible by 750.

- How do you test if a number is divisible by 5^n?

  Solution: See above.

Divisibility by 7

Problems

- Is 623 divisible by 7?

  Solution: $62 - 2 * 3 = 56$, and 56 is divisible by 7. So 623 is divisible by 7.

- Is $1,234,567,890$ divisible by 7?

  Solution: At each step we remove the last digit, double it, and subtract it from what remains.

  $$\begin{array}{r} 1234567890 \\ 123456789 \\ 12345660 \\ 1234566 \\ 123444 \\ 12336 \\ 1221 \\ 120 \\ 12 \end{array}$$

  So the number is not divisible by 7.

- Find a divisibility test for your favorite prime number.

  Solution: **See the website for a document about this.**

Divisibility by Powers of 10

Problems

- Is $1001^{10017} - 9812521809^2$ divisible by 10?

  Solution: Any number ending in 1, when raised to any power, still ends in a 1. Can you see why? Any number ending in 9, when squared, also ends in 1. So the difference of the two numbers above ends in 0. So it is divisible by 10.

- How many zeros are there at the end of the decimal representation of 25! ? If this number is written in binary (base 2), how many zeros are at the end of it? Can you think of a base in which this number has only 1 zero at the end of it?

  Solution Part 1: To know how many zeros 25! has, we need to know how many powers of 10 it is divisible by. To figure this out, let's make a list of all the integers ≤ 25 which are divisible by either 2 or 5, $\{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, 22, 24, 25\}$. Now, lets take this list and look at only the powers of 2 or 5 that it contains. The powers of two that each contains are $\{1, 2, 0, 1, 3, 1, 2, 1, 0, 4, 1, 2, 1, 3, 0\}$. So there are a total of 22 powers of 2. The powers of 5 that each of these number contain are $\{0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 2\}$. So the total number of powers of 5 is 6. The number $2^{22} * 5^6$ ends in 6 zeros. Can you see why? So 25! ends in 6 zeros.

  Solution Part 2: If a number is divisible by 2 but not 4, then in binary, it ends in a zero. If a number is divisible by 4 but not 8, then in binary it ends in 00. In general, if a number is divisible by 2^n but not 2^{n+1}, then in binary it end in a series of n zeros. Can you see why? Because we have shown that 25! is divisible by 2^{22} but ot 2^{23}, then in binary it ends in a series of 22 zeros. If we use the base 25!, then $(25!)_{25!} = 10$, which ends in one zero.

- If n is an integer, do n^5 and n always have the same last digit?

  Solution: They both have the same last digit if and only if $n^5 - n$ ends in 0, or in other words, $n^5 - n$ is divisible by 10. Let's check to see if this is true. If n is odd, then so is n^5. If n is even, then so is n^5. This shows that $n^5 - n$ is always even. Can you see why? So we only need t show that $n^5 - n$ is divisible by 5. By another problem below, $n^p - n$

is divisible by p whenever p is prime. Because 5 is prime, $n^5 - n$ is divisible by 5. We conclude that $n^5 - n$ is divisible by 10, so n^5 and n always end in the same last digit.

- Is there an integer, n, so that $(n-1)! + 1$ is divisible by 10?

  Solution: The number $(n-1)!$ always ends in zero for any $n \geq 6$. Can you see why? Because of this, $(n-1)!+1$ is not divisible by 10 if $n \geq 6$. So we only need to check the value of $(n-1)! + 1$ for $n = \{1, 2, 3, 4, 5\}$. The values are $\{2, 2, 3, 7, 25\}$, none of which are divisible by 10. So $(n-1)! + 1$ is never divisible by 10.

Divisibility by 11

Problems

- Is 1001 divisible by 11?

  Solution: $1 - 0 + 0 - 1 = 0$ which is divisible by 11, so 1001 is.

- Is $1,234,567,890$ divisible by 11?

  Solution $1 - 2 + 3 - 4 + 5 - 6 + 7 - 8 + 9 = 5$ which is not divisible by 11, so the number isn't either.

- Can the numbers $\{1, 2, 3, 4\}$ be arranged into a four digit number that is divisible by 11? What about the numbers $\{1, \ldots, 8\}$?

  Solution: Yes. $1 - 2 + 4 - 3 = 0$ which is divisible by 11, so 1243 is. The key to this was creating a sequence of $+1$ and -1 that canceled, $1-2+4-3 = -1+1 = 0$. Notice also that $1-2+4-3+5-6+8-7 = -1+1-1+1 = 0$. So 12435687 is divisible by 11. Can you find others?

- It's easy to see that 1133 is divisible by 11. Using this, show very quickly that 3113 and $1,001,003,003,000$ are also divisible by 11.

  Solution: Because $1 - 1 + 3 - 3$ is divisible by 11, this divisibility isn't effected if we just change the order of the two additions $3 - 1 + 1 - 3$. Also, notice that the paris of zeros in 1001003003000 don't effect the alternating sum of digits. So this number is divisible if 11330 is. But we know this is divisible by 11 because 1133 is.

- If a number has every one of its digits equal, under what conditions is that number divisible by 11?

  Solution: Suppose the number has n digits, all k's. If n is even, then $k - k + k - k + \ldots + k - k = 0$ is divisible by 11, so the number is. If n is odd, then $k - k + k - k + \ldots - k + k = k$ which is not divisible by 11. So a number whose digits are all the same is divisible by 11 if and only if it has an even number of digits.

More Problems and Extra Stuff

1. Prove that any product of k consecutive positive integers is divisible by k.

   Solution: Every other integer is divisible by 2. Every third integer is divisible by 3. And similarly, every kth integer is divisible by k. In other words, between two consecutive multiples of k there are exactly $k - 1$ integers which are not divisible by k. Suppose that we have a product of k consecutive integers, none of which are divisible by k. This would imply that between two consecutive multiples of k there were at least k integers not divisible by k. This is a contradiction, because there are only $k - 1$ such numbers. So any product of k consecutive integers is divisible by k because one of these integers is a multiple of k.

2. If n is any integer, prove that $n^2 + n$ is always divisible by 2, that $n^3 - n$ is always divisible by 3, and that $n^5 - 5n^3 + 4n$ is always divisible by 5. For a given prime number, p, can you find a polynomial expression like these that is always divisible by p?

   Solution: If we factor each of these polynomials we find,

$$\begin{aligned} n^2 + n &= n(n+1) \\ n^3 - n &= n(n^2 - 1) = (n-1)n(n+1) \\ n^5 - 5n^3 + 4n &= n(n^2 - 1)(n^2 - 4) = (n-2)(n-1)n(n+1)(n+2) \end{aligned}$$

   So these polynomials represent the products of 2, 3, and 5 consecutive integers, respectively. So by the previous problem, they are divisible by 2, 3, and 5 respectively, whenever n is an integer. These factorizations suggest a way to produce a polynomial which is divisible by any particualr prime p when n is an integer. Every prime > 2 is an odd number, $p = 2m + 1$. So we can form the polynomial

$$\begin{aligned} f(n) &= (n-m)\dots(n-1)n(n+1)\dots(n+m) \\ &= n(n^2-1)(n^2-4)\dots(n^2-m^2) \\ &= n^{2m+1} - (1+\dots+m^2)n^{2m} + \dots + (m!)^2 n \end{aligned}$$

3. Prove that $(p+1)^p - 1$ is divisible by p^2 if p is a prime number.

   Solution:

$$\begin{aligned} (p+1)^p - 1 &= \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} p^k - 1 \\ &= \sum_{k=1}^{p} \frac{p!}{k!(p-k)!} p^k \\ &= p \sum_{k=1}^{p} \frac{p!}{k!(p-k)!} p^{k-1} \\ &= p \sum_{k=0}^{p-1} \frac{p!}{(k+1)!(p-k-1)!} p^k \end{aligned}$$

   As proved below, $\frac{n!}{q!(n-q)!}$ is always an integer for $0 \le q \le n$. So each term in the series is an integer. But we can do better than this. By a problem above, $p!$ is divisible by p. So not only is $\frac{p!}{(k+1)!(p-k-1)!}$ an integer, but it is an integer divisible by p. Can you see why? So each term in the series is divisible by p. So $(p+1)^p - 1$ is divisible by p^2.

4. Prove that $n^p - n$ is divisible by p if p is a prime number. This is known as Fermat's Little Theorem.

   Solution: Notice that $1^p - 1 = 0$ is divisible by p. We now use induction. Suppose that $n^p - n$ is divisible by p for all $1 \le n \le N$. Then

$$\begin{aligned} (N+1)^p - (N+1) &= \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} N^k - (N+1) \\ &= \sum_{k=1}^{p} \frac{p!}{k!(p-k)!} N^k - N \\ &= \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} N^k + (N^p - N) \end{aligned}$$

As we have shown in other problems, the terms in the series are all integers divisible by p. Therefor the entire series is divisible by p. Also, we know that $N^p - N$ is divisibly by p. This shows that $(N+1)^p - (N+1)$ is divisible by p. So by induction $n^p - n$ is divisible by p for all $1 \leq n$.

The Binomial Theorem

Problems

- Check that $\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}$.

  Solution:

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

- Use the previous problem (and induction) to show that the coefficients in the binomial expansion $\left(\frac{n!}{k!(n-k)!}\right)$ are always integers.

  Solution: Define $C(n,k) = \frac{n!}{k!(n-k)!}$. Obviously $C(1,0) = C(1,1) = 1$ are both integers. As are $C(2,0) = C(2,2) = 1$ and $C(2,1) = 2$. Let us assume that $C(n,k)$ is an integer for all $1 \leq n \leq N-1$ and for $0 \leq k \leq n$. This implies that $C(N-1, k-1) = \frac{(N-1)!}{(k-1)!(N-k)!}$ and $C(N-1,k) = \frac{(N-1)!}{k!(N-k-1)!}$ are integers for $1 \leq k \leq N-1$. So their sum is also an integer. But, by the previous problem, their sum is $C(N,k)$. So $C(N,k)$ is also an integer for all $1 \leq k \leq N-1$. To complete the induction, we notice that $C(N,0) = C(N,N) = 1$ which are also integers. Thus $C(n,k)$ is an integer for all $1 \leq n \leq N$ and $0 \leq k \leq n$. So by induction, $C(n,k)$ is an integer for all $1 \leq n$ and $0 \leq k \leq n$.