Intro to Number Theory: Why your calculator and Homer Simpson are sometimes wrong.

Dr. David M. Goulet

November 14, 2007

Intro

The Pythagorian Theorem says that if a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse, then $a^2+b^2 = c^2$. This equation has some well known integer solutions. For example $3^2 + 4^2 = 5^2$.

Fermat's last theorem says that if you replace the exponent 2 with any larger integer, there are no positive integer triples, a, b, and c which satisfy the equation. For example, Fermat's last theorem[1] says there are no positive integer solutions to $a^3 + b^3 = c^3$.

The Simpsons had an episode which seemed to offer a contradiction to Fermat's theorem. During The Simpsons' 1995 Halloween special the equation $1782^{12} + 1841^{12} = 1922^{12}$ floated through the air over Homer's head[2].

[1]Although Fermat claimed to have proved this theorem, he never showed anyone the proof (if it existed). This theorem took over 350 years to prove and frustrated some of the world's greatest mathematicians, including Leonard Euler. Rumor has it that Euler was so frustrated trying to prove the theorem that, after Fermat died, Euler had his house torn apart, looking for a scrap of paper that might contain the proof which could have fallen through the floor boards. Around 1994, Andrew Wiles at Princeton proved the theorem in an indirect and innovative way. It took him over 200 pages and 7 years.

[2]For more details about this Simpson's episode, see the following link. http://www.sciencenews.org/articles/20060610/bob8.asp

Your Calculator will tell you that $\sqrt[12]{1782^{12} + 1841^{12}} = 1922$. Is this a contradiction to the theorem? You'll soon be able to prove that your calculator and Homer are wrong.

Preliminaries

Base 10 Arithmetic

An integer can be represented in base k by a string of digits $d_n d_{n-1} \ldots d_1$. That is $d_n d_{n-1} \ldots d_1 = d_n k^{n-1} + d_{n-1} k^{n-2} + \ldots + d_1 k^0$. For example, in base 10

$$54321_{10} = 5 * 10^4 + 4 * 10^3 + 3 * 10^2 + 2 * 10 + 1$$

while in base 7

$$\begin{aligned} 54321_7 &= 5 * 7^4 + 4 * 7^3 + 3 * 7^2 + 2 * 7 + 1 \\ &= (12005 + 1372 + 147 + 14 + 1)_{10} \\ &= 13539_{10} \\ &= 10^4 + 3 * 10^3 + 5 * 10^2 + 3 * 10 + 9 \end{aligned}$$

Computers sometimes use base 16, known as hexidecimal notation. The letters A, B, C, D, E, F are used to represent the digits larger than 9 in base 16. For example

$$\begin{aligned} 9A7E_{16} &= 9 * 16^3 + 10 * 16^2 + 7 * 16 + 14 \\ &= 39550_{10} \end{aligned}$$

Problems

- What is $7777 + 1$ in base 8?
- In what base is 21^2 equal to 225_{10} ?
- 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? (Use a calculator.)

Fundamental Theorem of Arithmetic

Greek geometer Euclid (circa 300 B.C.) had an idea that Carl Friedrich Gauss proved as a theorem in 1801. The fundamental theorem of arithmetic says that each positive integer can be factored uniquely into powers of primes. That is, for every $n \in \mathbb{Z}^+$, there is a unique set of primes $\{p_1, \ldots, p_r\}$ and a uniques set of integers $\{m_1, \ldots, m_r\}$ such that $n = p_1^{m_1} \ldots p_r^{m_r}$. For example

$$\begin{aligned} 36 &= 2^2 * 3^2 \\ 340 &= 2^2 * 5 * 17 \\ 7168 &= 2^{10} * 7 \end{aligned}$$

$\sqrt{2}$ is irrational. We'll prove that $\sqrt{2}$ is irrational. Suppose that it is rational, then there exist two integers with no common divisor so that $\sqrt{2} = p/q$. This shows $2q^2 = p^2$.

Obviously both sides are integers. Because 2 is a factor of the left side, by the theorem, it is a factor of the right side. So, p^2 is divisible by two. But, by the theorem, p has a unique factorization $r_1^{m^1} \ldots r_k^{m^k}$ and so does p^2. So p^2 has the unique factorization $r_1^{2m_1} \ldots r_k^{2m_k}$. Thus, if p^2 is divisible by 2, then so is p and so p^2 is actually divisible by 4.

So the left side must also be divisible by 4. Namely, q^2 must be divisible by 2, but then the theorem implies that q is divisible by 2, a contradiction to the fact that p and q have no common factors.

Problems

- Factor 120 uniquely into primes.
- Three integers (x, y, z) satisfy $34x + 51y = 6z$. If y and z are primes, what are these numbers?
- Prove that $\sqrt{p}$ is an irrational number for any prime p.
- Suppose that p is the largest prime number. Is $p! + 1$ divisible by any primes $\leq p$? Is this a contradiction?

Divisibility Tests

Divisibility by Powers of 2

An integer is divisible by 2 if and only if it's last decimal digit is divisible by 2.

Proof: Write n in decimal notation as the string of digits $d_k d_{k-1} \ldots d_2 d_1$. We can write

$$n = 10 * (d_k \ldots d_2) + d_1$$

Now, if n is divisible by 2, then, because 10 is divisible by 2, d_1 must also be. Also, if d_1 is divisible by 2, then because 10 is also, n is divisible by 2.

An integer is divisible by 2^n if and only if its last n digits, used to create a new n digit number, result in a number that is divisible by 2^n. For example, 123456 is divisible by 8 because 456 is.

Problems

- Is $1,234,567,890$ divisible by 2?
- Is $121^{13} - 101^4$ divisible by 2?
- Prove that $1782^{12} + 1841^{12} \neq 1922^{12}$. Do you know why your calculator is wrong?
- How do you prove the 2^n case?

Divisibility by 3 and 9

An integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3. An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Proof: Write n in decimal notation as $d_k \ldots d_1$.

$$\begin{aligned} n &= 10 * (d_k \ldots d_2) + d_1 \\ &= 9 * (d_k \ldots d_2) + 10 * (d_k \ldots d_3) + d_2 + d_1 \\ &= 9 * (d_k \ldots d_2) + 9 * (d_k \ldots d_3) + 10 * (d_k \ldots d_4) + d_3 + d_2 + d_1 \\ &= 9 * (d_k \ldots d_2) + \ldots + 9 * d_k + (d_k + d_{k-1} + \ldots + d_2 + d_1) \end{aligned}$$

Each of the first $k-1$ terms is obviously divisible by 3, so by the same reasoning as the proof of divisibility by 2, the sum $d_k + \ldots + d_1$ is divisible by 3 if and only if n is divisible by 3.

Problems

- Does the above proof also work for the case of divisibility by 9?
- Is $1,234,567,890$ divisible by 3?
- Is $326^2 - 325^2$ divisible by 3?
- Is $65,314,638,792$ divisible by 24?

Divisibility by Powers of 5

An integer is divisible by 5 if and only if its last decimal digit is divisible by 5.

Proof: Again let n be written in decimal form as $d_k \ldots d_1$.

$$n \quad = \quad 10 * (d_k \ldots d_2) + d_1$$

By the same reasoning as in above proofs, n is divisible by 5 if and only if d_1 is divisible by 5.

Problems

- Is $1,234,567,890$ divisible by 5?
- How many 3 digit numbers are divisible by 5?
- Find a divisibility test for 125. Use your test to decide if $1,234,567,890,000$ is visible by 750.
- How do you test if a number is divisible by 5^n?

Divisibility by 7

An integer is divisible by 7 if and only if removing the last digit and subtracting two of it from the result gives a number that is divisible by 7.

Proof: Let n have the decimal representation $d_k d_{k-1} \dots d_2 d_1$. Then $n = 10 * (d_k \dots d_2) + d_1 = 7 * (d_k \dots d_2 + d_1) + 3 * (d_k \dots d_2 - 2 * d1)$. By the same reasoning as previous proofs, 7 divides n iff it divides $d_k \dots d_2 - 2 * d1$.

Others The proof of the divisibility test for 7 leads to a divisibility test for any prime. For example, to find a divisibility test for 13, we write n in decimal form as $d_k d_{k-1} \dots d_2 d_1$. Then we rewrite this.

$$d_k \dots d_1 = 13 * (d_k \dots d_2 + d_1) - 3 * (d_k \dots d_2 + 4 * d1)$$

So, to check for divisibility by 13 we remove the last digit, multiply it by 4, and then add it to what remains. For example $1,234,567,890$ is not divisible by 13.

1234567890
123456789
12345714
1234587
123486
12372
1245
144
30
3

Obviously these tests are not always practical.

Problems

- Is 623 divisible by 7?
- Is $1,234,567,890$ divisible by 7?
- Find a divisibility test for your favorite prime number.

Divisibility by Powers of 10

Count the zeros!

Problems

- Is $1001^{10017} - 9812521809^2$ 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?
- If n is an integer, do n^5 and n always have the same last digit?
- Is there an integer, n, so that $(n-1)! + 1$ is divisible by 10?

Divisibility by 11

An integer is divisible by 11 if and only if the alternating sum of its digits is.

Proof: The proof is similar to the case of 3.

$$\begin{aligned} n &= 10 * (d_k \dots d_2) + d_1 \\ &= 11 * (d_k \dots d_2) - 10 * (d_k \dots d_3) - d_2 + d_1 \\ &= 11 * (d_k \dots d_2) - 11 * (d_k \dots d_3) + 10 * (d_k \dots d_4) + d_3 - d_2 + d_1 \\ &= 11 * (d_k \dots d_2) - \dots + (-1)^k 11 * d_k + (d_1 - d_2 + \dots + (-1)^k d_k) \end{aligned}$$

By the same reasoning as previous cases, n is divisible by 11 if and only if $d_1 - d_2 + d_3 - \dots$ is. For example $1,234,567,890$ is not divisible by 11 because $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$ and 5 isn't divisible by 11.

Problems

- Is 1001 divisible by 11?
- Is $1,234,567,890$ divisible by 11?
- Can the numbers $\{1, 2, 3, 4\}$ be arranged into a four digit number that is divisible by 11? What about the numbers $\{1, \dots, 8\}$?

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

More Problems and Extra Stuff

These problems don't necessarily use the tests given above, but they are still fun to think about.

1. Prove that any product of k consecutive positive integers is divisible by 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?
3. Prove that $(p+1)^p-1$ is divisible by p^2 if p is a prime number.
4. Prove that n^p-n is divisible by p if p is a prime number. This is known as Fermat's Little Theorem.

Problems 2 and 3 can be solved by making use of the binomial theorem, described below.

The Binomial Theorem You've probably seen these.

$$\begin{aligned}(x+1)^2 &= x^2+2x+1\\ (x+1)^3 &= x^2+3x^2+3x+1\end{aligned}$$

Which are special cases of this.

$$(x+1)^n=\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}x^k$$

Which is a special case of this.

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

Proof. Obviously it is true for $n = 1, 2, 3$. Induction

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

For example $1 + \frac{4!}{3!1!} + \frac{4!}{2!2!} + \frac{4!}{1!3!} + 1 = (1+1)^4 = 16$.

The ideas in the theorem may have been known as early as 300 B.C., but it was proved in great generality by Isaac Newton in the 1600's. Newton proved that it is still true in some sense even if n is not an integer.

Problems

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

We'll prove that $(p+1)^p - 1$ is divisible by p.

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

Each term in the sum is an integer (why?) so the sum is an integer and $(p+1)^p - 1$ is divisible by p. It's actualy possible to show that this number is divisible by p^2 (see problem above).