

Prime Factorization and Digit Congruence

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-07/4364.html>

From: Ross A. Finlayson (raf_at_tiki-lounge.com)

Date: 07/17/04

Date: 16 Jul 2004 22:17:21 -0700

A funny joke:

There are two groups of people in the world:
Those who can be categorized into one of two
groups of people, and those who can't.

<http://www.workjoke.com/projoke22.htm>

The statement must be false, for it claims to not be able to achieve its claim.

I was interested the other day to read mention of testing decimal numbers for divisibility by seven, in summing each odd group of three digits as a decimal number and subtracting the sum of each even group of three digits as a decimal number.

It reminds me of the case of "casting nines" or "casting out nines", where a decimal number that has digits that sum to a multiple of nine is a multiple of nine.

Also mentioned was a method for eleven, the same method as for seven. Dissimilarly for eleven it is not necessary to group the digits to consider a higher base but only to alternately add and subtract the digits and test for divisibility.

I figure it would be worthwhile to apply that as a method to factorize fall primes from an arbitrary number represented as a bitstring, in addition to the method of factoring twos by counting the number of least significant zeros and factoring the Mersenne numbers using digit summation congruence. Yet, while I have a clue that the digit summation congruence for base b can be used as a test for the factor $b-1$, or one of its roots, for testing as factors the Mersenne numbers 2^n-1 , I need better understanding of this method for sevens and elevens in base ten if I am to apply it to the easily tractable bases in binary: two, four, eight, sixteen, etcetera, 2^n .

In decimal, three digits in the first three integral moduli from zero (or "orders of magnitude") allows a range from 0 to 999. Neither

sci.math: Prime Factorization and Digit Congruence

seven nor eleven divides into a thousand. $1000\%7$, $1000 \bmod 7$, the remainder of even division of 1000 by 7, = 6, $1000\%11 = 10$. So in the case of those numbers seven and eleven, x , for base $b=10$, $b^3 \% x = x-1$.

In base 8, 8^3 is 512. There do not seem to be many numbers x near 8 that $512\%x=x-1$. Perhaps 16, 2^4 , will have an easier example. Sixteen cubed is $2^4 \cdot 2^3 = 2^7 = 128$ or 4096, in looking for x s.t. $b^3 \% x = x-1$.

This is where I am thinking that the fact that $b^3 \% x = x-1$ is the reason this method appears to work as digit summation, in this case alternating grouped digit summation and subtraction, offers a factorization test for small primes.

We discussed the case of $b-1$ and its roots that is used for the Mersenne numbers in the thread "A INTRACTABLE problem on PRIMES." I implemented and described toy software using this method in a few posts of "Factorial/Exponential Identity, Infinity", Mersenne Digit Summation Congruence, DSC.

Here's a decent exposition:

<http://www.mathpages.com/home/kmath269/kmath269.htm>

The idea is to use this method with the computer's very rapid and efficient binary arithmetic to produce algorithms in the bases that are a power of two. The large composites to be tested for these small factors are sequences of tens to hundreds to thousands of bits, and it's simple to operate on them particularly in groups of eight bits, bytes, base $2^8 = 256$. Instead of, say, actually dividing the huge number using extended precision arithmetic to see if there is a remainder, the Mersenne numbers can be more rapidly determined to be factors, and then division results. It's efficient for us, too, determining if a decimal number is a multiple of nine is as simple as summing its digits, and that sum, recursively, until a known multiple of nine is recognized.

So I wonder about seven and eleven in decimal, and how to apply a similar method for "a base that is a power of two".

What's a word that's an adjective describing a number being a power of two? That's to ask, as example "of two" is binary or binal, "of four" quaternary or quaternal, "of sixteen" hexadecimal or sexadecimal, what's the general term for "of a power of two"? That would be convenient instead of continually grammatically structuring "of any power of two" in use.

>From MathWorld, "Divisibility Tests":

<http://mathworld.wolfram.com/DivisibilityTests.html>

sci.math: Prime Factorization and Digit Congruence

There are some more methods described for divisibility and congruence.

I have in mind to design further algorithms to use a variety of divisibility tests to test factors of tracts of binary digits of large composites, as I develop some factorization software.

I had this in mind in determining some of the ways that Stirling numbers always are integers, analysis tools, because I want to understand more about the rational functions that comprise some Stirling numbers, and analytical forms of those, towards some better understanding of some of the other contents of the "Factorial/Exponential Identity, Infinity" thread.

Besides that, they're high performance factorization algorithms suitable for pre-treatment of numbers before the factorized result is sent to elliptic curve or other modern, memory-intensive, methods of integer factorization.

Regards,

Ross F.