Number Theory # 2

Factoring

In the last homework problem, it takes many steps of the Euclidean algorithm to find that the gcd of the two numbers is 1. However, if we had initially observed that 11384623=5393*2111, then we could have easily checked by long division that neither 5393 nor 2111 were factors of 2110800204 and we would have prove that the gcd of the two numbers was 1 very easily. Of course, observing that $11384623 = 5393 \times 2111$ is the tricky part.

In today's world, factoring large numbers is a very important problem. The reason it is so important is largely due to its application in cryptography. The basis of many encryption systems is that it is very easy for you to pick two large numbers a and b and multiply them together to get x, but very difficult for someone to take x and figure out what numbers a and b you multiplied together. In fact, RSA Laboratories was offering large cash prizes (up to $200,000) for the first person to factor certain numbers. However, they stopped offering the prizes in 2007.

The reason for offering the prizes was to try to understand how easy it would be for people to factor these certain large numbers. For example, of how much this area of mathematics was improved over the last 35 years, in 1976 Martin Gardner wrote that the 129 digit RSA challenge number would not be factored for 40 quadrillion years... but, it was factored by Arjen Lenstra in 1994. In December 2009, the 768 digit RSA challenge number was factored. The 2048 digit number still hasn't been factored yet, so you still have something to work on.

However, the problem of factoring numbers in primes has always been of interest to mathematicians. There is a famous case of Professor Cole, giving a presentation in 1903 in which, without ever saying a word, he proceeded to calculate $2^{67} - 1$ by hand, and then multiplying $193707721 \times 761838257287$ by hand and showing they were equal. Another famous case is in the 1630s Mersenne asked Fermat if he thought 100895598169 was prime. After a short period, Fermat replied that it was the product of 898423 and 112303. Nobody knows how he did it, and some people wonder if he had a factoring algorithm that he did not share which has not yet been rediscovered.

We will now look at a couple of ways of factoring numbers.

Trial Division

As you know, the most basic way of factoring a number n is to start trying to divide n by all prime numbers up to $\sqrt{n}$. For small numbers this can be effective, especially if we have some tricks to help us:

Divisibility by 2?

Check if units digit is even.

Divisibility by 3?

Find the sum of the digits. Check if this sum is divisible by 3.

Example: 247392479372: 2+4+7+3+9+2+4+7+9+3+7+2=59=5+9=14 is not divisible by 3 so 247392479372 is not divisible by 3.

Divisibility by 5?

Check if the units digit is 0 or 5.

Divisibility by 11?

Find the alternating sum of the digits. Check if this alternating sum is divisible by 11.

Example: 582482957243: 5-8+2-4+8-2+9-5+7-2+4-3=11, so it is divisible by 11.
Divisibility by 7?

Start with the integer, remove the units digit and subtract 2 times this units digit from the number that is left. Repeat until you get a small number and check if this is divisible by 7.

Example: 18767: 1876 - 2(7) = 1862

186 - 2(2) = 182

18 - 2(2) = 14

which is divisible by 7. Therefore, 18767 is divisible by 7.

Divisibility by 13?

Use the method for 7, but add 4 times the units digit instead of subtracting 2 times the units digit.

Example: 421616: 42161+4(6)=42185

4218+4(5)=4238

423+4(8)=455

45+4(5)=65

which is divisible by 13. Therefore, 421616 is divisible by 13.

EXERCISE Prove the following numbers are composite by finding a prime factor.

70272753, 2663683, 304603, 32821.

Solution:

1. $7+0+2+7+2+7+5+3=33$ which is divisible by 3, so 3 is a factor of 70272753.
2. $2+6+6+3+6+8+3=34$ so it is not divisible by 3. But, $2-6+6-3+6-8+3=0$, so 11 is a factor.
3. We find that 3, 11, and 7 are not factors, but 13 is a factor because

$$\begin{aligned} 30460+4(3) &= 30472 \\ 3047+4(2) &= 3055 \\ 305+4(5) &= 325 \\ 32+4(5) &= 52 \\ 5+4(2) &= 13 \end{aligned}$$

4. Using our methods above, we find that 32821 is not divisible by 2, 3, 5, 7, 11, or 13. What now? We try the next few primes using long division. We find that 17 and 19 are not factors, but $32821 = 23 \times 1427$.

EXERCISE Find the prime factorization of 663993.

Solution: From our divisibility for 3 trick, this is clearly divisible by 3. We get by division $663993 = 3 \times 221331$.

We have $2+2+1+3+3+1=12$, so it is divisible by 3. We get $221331 = 3 \times 73777$.

Now $7+3+7+7+7=31$, so it is not divisible by 3. But, $7-3+7-7+7=11$ so it is divisible by 11. $73777 = 11 \times 6707$.

We already know 6707 is not divisible by 3 as 73777 wasn't. So, we check 11, 13, 17, and then find 19 is a factor. We get $6707 = 19 \times 353$. What about 523? Since $19^2 = 361$, and we know that it is not divisible by a prime less than 19, it must be prime. Thus, $663993 = 3^2 \times 11 \times 19 \times 353$.

This method works very poorly if all of the prime factors of a number are very large. The worst case would be for a number like $39203 = 197 \times 199$ (note that 197 and 199 are both prime). We would have had to check 45 primes before we found a single factor, and the number is only 5 digits long! We now look at another factoring algorithm invented by Fermat, which will actually check for large factors that are close together.

Fermat's Algorithm

We know that $(a-b)(a+b) = a^2 - b^2$. Thus, given any number n if we can find a number a such that $a^2 - n$ is a perfect square, then we can write $a^2 - n = b^2$ so $n = a^2 - b^2 = (a+b)(a-b)$. We use the following algorithm.

Algorithm To fact a large positive integer n, pick the smallest integer k such that $k^2 > n$. Find the first number in the sequence

$k^2 - n$, $(k+1)^2 - n$, $(k+2)^2 - n$, ...,

that is a perfect square, say $(k+m)^2 - n = b^2$. Then, $n = (k+m)^2 - b^2 = (k+m+b)(k+m-b)$.

EXAMPLE Use Fermat's Algorithm to factor 1073 and 931.

Solution: We can find that $33^2 = 1089$. We find that

$$33^2 - 1073 = 1089 - 1073 = 16 = 4^2$$

so $1073 = 33^2 - 4^2 = (33+4)(33-4) = 37 \times 29$.

For 931, we find that $31^2 = 961$, and

$$\begin{aligned} 31^2 - 931 &= 30 \\ 32^2 - 931 &= 93 \\ 33^2 - 931 &= 158 \\ 34^2 - 931 &= 225 = 15^2 \end{aligned}$$

Thus, $931 = 34^2 - 15^2 = (34+15)(34-15) = 49 \times 19$.

EXERCISE Use Fermat's Algorithm to factor the following numbers: 713, 1763, 851, 533.

Solution: We have $27^2 = 729$. We find that $27^2 - 713 = 16 = 4^2$, so $713 = (27+4)(27-4) = 31 \times 23$

We have $42^2 = 1764$, so $42^2 - 1764 = 1^2$. Thus, $1764 = 43 \times 41$.

We have $30^2 = 900$ and $900 - 851 = 49$, so $851 = (30+7)(30-7) = 37 \times 23$.

We have $24^2 = 576$. We find

$$\begin{aligned} 24^2 - 533 &= 43 \\ 25^2 - 533 &= 92 \\ 26^2 - 533 &= 143 \\ 27^2 - 533 &= 196 = 14^2 \end{aligned}$$

Thus, $533 = (27+14)(27-14) = 41 \times 13$.

Observe that the worst case for Fermat's Algorithm is when the factors of n are far apart. As a side note, if Fermat used this method to factor 100895598169, it would have taken 75419 iterations before he got to

$$393060^2 - 100895598169 = 505363^2$$

So, he probably did it another way... but how?!?

A Table of Squares:

x	x^2	x	x^2
1	1	21	441
2	4	22	484
3	9	23	529
4	16	24	576
5	25	25	625
6	36	26	676
7	49	27	729
8	64	28	784
9	81	29	841
10	100	30	900
11	121	31	961
12	144	32	1024
13	169	33	1079
14	196	34	1156
15	225	35	1225
16	256	36	1296
17	289	37	1369
18	324	38	1444
19	361	39	1521
20	400	40	1600

Problems

1. Prove the following numbers are composite by finding a prime factor.
   (a) 1517
   (b) 37023
   (c) 213697
   (d) 3599
   (e) 2499
   (f) 2479
2. Find the prime factorization of the following numbers.
   (a) 30030
   (b) 8091
   (c) 61997