4. Remarks on primes and some excercises

1) Find integers x and y such that $423x+198y=9$.
2) Prove that $4 \nmid n^2+2$ for each $n \in \mathbb{Z}$.
3) Prove that for each $n \in \mathbb{Z}$, $2 \mid n^2-n$; $6 \mid n^3-n$, $5 \mid n^5-n$.
4) Prove that $(1+n!, 1+(n+1)!)=1$ for each $n \in \mathbb{N}$.
5) If $m, n \in \mathbb{N}$, then $(a^{2^n}-1) \mid (a^{2^m}-1)$ if $m \geq n$.
6) If $a, m, n \in \mathbb{N}$, $m \neq n$, then $(a^{2^m}+1, a^{2^n}+1) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}$
7) (Mersenne primes) Show that if 2^n-1 is a prime, then n is prime and not conversely.

A prime of the form 2^p-1, p a prime, is called a Mersenne prime (after Father Marin Mersenne (1588-1648). It is known that 2^p-1 is a prime for $p \in \{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127\}$.
The largest Mersenne prime known by (2015): 2^{756839}

It is conjectured that the number of Mersenne primes is infinite.

8) Show that there are no positive integers $a, b,$ such that $(a^n - b^n)$ divides $(a^n + b^n)$ for $n > 1$. Use this to prove that $2^n + 1$ is a prime only if n is a power of 2.

9) Recall: the n^{th} Fermat number F_n is $2^{2^n} + 1$ $(n > 0)$ and $F_0 = 3$. As F_n rapidly grows as n increases, compositeness of F_n was settled (by hand) only for $n = 6$ in 1880 by F. Landry, for $n = 7$ in 1905 by J. C. Morehead and A. E. Watson, for $n = 8$ in 1980 by Brent and Pollard. After the advent of computer calculations, compositeness of F_n is known for $5 \leq n \leq 32$. Compositeness of F_{33} remains to be determined.

An aside in deciding the compositeness of F_n's.

Theorem. Any prime divisor ~~of~~ p of F_n is of the form $(n \geq 2)$: (i) $p = k\,2^{n+1}+1$ (Euler 1747);
(ii) $p = k.\,2^{n+2}+1$ (E. Lucas 1879).
(i.e., k in (i) is even.)

The numbers ~~of~~ of the form $k\,2^n+1$ are of considerable interest:

(i) The smallest integer n (for a given k) such that $k\,2^n+1$ is prime may be very large. For $k=47$, $n=583$ is the smallest integer such that $k \times 2^n+1$ is a prime.

(ii) There exist an infinite number of odd integers k for which $k \times 2^n+1$ is composite for all $n \geq 1$.

The problem of determining least such k

is open. up to now, $K = 78557$ is the smallest ~~prime~~ known K for which $K.2^n+1$ is never a prime for any n.

Problem (cont'd)

10) use $5 \times 2^7 \equiv -1 \pmod{641}$ to show that $641 \mid F_5$

11) Show that $2^{2^n}-1$ has at least n primes. In particular, the number of primes is infinite. (Hint: $(2^{2^n}-1) = (2^{2^{n-1}}-1)(2^{2^{n-1}}+1)$. Use induction)

12) Show that $2^{58}+1$ is composite. (Hint: use the identity $4x^4+1 = (2x^2-2x+1)(2x^2+2x+1)$.

13) Show that the last digit of F_n is 7 for all $n \geq 2$. Deduce that F_n can never be a perfect square. (Hint: $2^{2^n} \equiv 6 \pmod{10}$ for all $n \geq 2$)

4.5

4.1) More about primes. We saw that the set P of primes is infinite. A search for their distribution among the natural number is eluded so far. Whether any pattern exists is so far not clear. Some aspects we have so far unearthed is very fascinating and has deep connections with other aspects of mathematics.

As we go along, some elementary and accessible aspects will be studied and some open problems will be indicated.

One very striking aspect is that some simply stated and understandable problems have very complicated solutions or have resisted solutions over decades, some times centuries.

For some, existance of a solution with in the number systance can be decided or not is also a major problem.

A major motivation to pursue the effort to solve them, apart from curiosity, is that it may ~~wa~~ lead to new aspects of the structure of numbers and connections to other mathematical aspects.

Gaps between primes

Though the gaps between odd primes can be as small as possible (ex., 3 and 5, 11 and 13, etc.), it can be arbitrarily large. For example, for each $k \in \mathbb{N}$, $(k+1)!+2, (k+1)!+3, \dots, (k+1)!+(k+1)$ are all composite because $j \mid (k+1)!+j$ for all j, $2 \leq j \leq k+1$.

A famous problem in this direction is a solution to
Twin prime conjecture: There exist an infinite number of pairs $(P, P+2)$ of prime numbers.

Ex: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, ...

The largest twin primes known is ~~2,996,863,034,89~~
$\pm 1 + 2,996,863,034,895 \times 2^{1290000}$.

A major progress on this conjecture was made by the chinese mathematician Yitang 'Tom' Zhang (2014): There are infinitely many pairs of primes that differ by 70 million or less.

More precisely: For $n \in \mathbb{N}$, $n \geq 2$, let $\hat{P}(n)$ stand for the statement: « there are an infinite number of pairs of primes that differ exactly by n. »

The twin prime conjecture is that $\hat{P}(2)$ holds.

Zhang proved that: there exists an integer $K < 70{,}000{,}000$ such that $P(K)$ holds; i.e., if $p(n)$ is the n^{th}-prime, then

$$\liminf_{n \to \infty} (p_{n+1} - p_n) \leq 7 \times 10^7$$

This is a qualitative result: its main content is the existance of a finite bound K such that there exist infinite number of primes p_n, p_{n+1} with a difference K.

A project undertaken by a group of Mathematicians ('polymath') lead by Terrance Tao and Maynard shows that $K < 246$. If 'generalized Riemann hypothesis' is true, then $K \leq 6$.

The following recent conjecture seems to have many applications.

(a, b, c)-Conjecture (Joseph Osterle (1988) and David Masser (1985))

For a positive integer n, let rad(n) (read as radical of n) denote the product of distinct prime divisors of n.

Conjecture: i) There exists an infinite number of triples of integers (a, b, c) which are ~~coprime~~ coprime such that: $c = a + b$ and $\mathrm{rad}(abc) > c$.

(ii) ~~I.o.w.~~ For each $\varepsilon > 0$, there exist finitely many triples a, b, c of coprime integers such that $a + b = c$ and $c > \mathrm{rad}(abc)^{1+\varepsilon}$

i.e., the product of distinct primes dividing abc is ~~not~~ usually not smaller