November 9 – 19, 2021. Limbe (Cameroun)

Number Theory
II: Prime Numbers
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Assignment 2

1. Let $a \geq 2$ and $n \geq 2$ be two integers. Assume that $a^n - 1$ is prime. Show that $a = 2$ and that n is prime.

2. Let $a \geq 2$ and $n \geq 2$ be two integers. Assume that $a^n + 1$ is prime. Show that a is even and that n is a power of 2.

Give an example of a pair (a, n) where a is an integer ≥ 3 which is not a power of 2 and n is an integer ≥ 2 such that $a^n + 1$ is prime.

3. Let a, m, n be positive integers with $m \neq n$. Show that the gcd of $a^{2^m} + 1$ and $a^{2^n} + 1$ is 1 is a is even, and is 2 if a is odd.

4. Let $a \geq 2$ and $n \geq 1$ be integers. Let p be an odd prime divisor of $a^{2^n} + 1$. Show that p is congruent to 1 modulo 2^{n+1}.

Deduce that for each $n \geq 1$, there are infinitely many primes p congruent to 1 modulo 2^{n+1}.

5. Using $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$, show that 641 divides $2^{32} + 1$.

6. Let $f \in \mathbb{Z}[X]$ be a non constant polynomial.
(a) Show that the set

$$\{p \mid p \text{ prime, there exists an integer } n \geq 0 \text{ such that } p \text{ divides } f(n)\}$$

is infinite.
(b) For $m \geq 2$, denote by $P(m)$ the largest prime factor of m; set also $P(0) = 0$, $P(1) = 1$ and $P(-m) = P(m)$. Check

$$\limsup_{n \to +\infty} P(f(n)) = \infty.$$

November 9 – 19, 2021. Limbe (Cameroun)

Number Theory
II: Prime Numbers
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Assignment 2 — Solution

(1). Write

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Since $a \geq 2$ and $n \geq 2$ we have $a^{n-1} + a^{n-2} + \cdots + a + 1 > 1$. Hence if the number $a^n - 1$ is prime, then $a - 1 = 1$, and $a = 2$.

Assume $n = kd$ with $d > 1$. Set $b = 2^k$ and write

$$2^n - 1 = b^d - 1 = (b-1)(b^{d-1} + b^{d-2} + \cdots + b + 1),$$

so that $2^n - 1$ is divisible by $b - 1$; since $1 \leq b - 1 < 2^n - 1$ and since $2^n - 1$ is prime, we deduce $b - 1 = 1$, $2^k = 2$ and $k = 1$, $d = n$. Hence n is prime.

The prime numbers of the form $2^p - 1$ are called the *Mersenne primes*.

(2). Assume $d \geq 3$ is an odd divisor of n. Write $n = kd$, $b = a^k$ and

$$a^n + 1 = b^d + 1 = (b+1)(b^{d-1} - b^{d-2} + \cdots - b + 1).$$

Hence $b + 1$ divides $a^n + 1$. This is not compatible with the assumption that $a^n + 1$ is prime because $1 < b + 1 < a^n + 1$. Therefore n has no odd prime divisor, which means that n is a power of 2.

The prime numbers of the form $2^{2^n} + 1$ are called the *Fermat primes*.

`Remark`. For $a = 6$ and $n = 2$ the number $6^2 + 1 = 37$ is prime. It is conjectured that $x^2 + 1$ is prime for infinitely many positive integer x. The first primes of the form $n^2 + 1$ are

$$2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, \ldots$$

`https://oeis.org/A002496` and the corresponding values of n are

$$1, 2, 4, 6, 10, 14, 16, 20, 24, 26, 36, 40, 54, 56, 66, \ldots$$

https://oeis.org/A005574

An example with $n = 4$ and $a^n + 1$ prime is with $a = 6$.

(3). (This is [1] Exercise IV.3). Without loss of generality assume $m > n$. Let $k = m - n$. Set $x = a^{2^n}$, so that $a^{2^m} = x^{2^k}$. Since $k \geq 1$, $x + 1$ divides $x^{2^k} - 1$. Hence $a^{2^n} + 1$ divides $a^{2^m} - 1$.

If d divides both $a^{2^m} + 1$ and $a^{2^n} + 1$, it divides $a^{2^m} + 1$ and $a^{2^m} - 1$, hence it divides the difference which is 2. Therefore the gcd of $a^{2^n} + 1$ and $a^{2^m} + 1$ is 1 or 2. Finally these numbers are even if and only if a is odd.

(4). (This is [1] Exercise VIII.3). If n and a are positive integers and p an odd prime such that a^{2^n} is congruent to -1 modulo p, then the class of a modulo p in the group $(\mathbb{Z}/p\mathbb{Z})^\times$ has order 2^{n+1}, hence 2^{n+1} divides $p - 1$ and p is congruent to 1 modulo 2^{n+1}.

Let $p_1, \ldots, p_s$ be primes which are congruent to 1 modulo 2^{n+1}. Let m be the largest integer such that 2^m divides $p_i - 1$ for $1 \leq i \leq s$; hence $m \geq n+1$. Let p be an odd prime which divides $a^{2^m} + 1$. Then p is congruent to 1 modulo 2^{m+1}, hence p is congruent to 1 modulo 2^{n+1} and is different from $p_1, \ldots, p_s$.

5. From (4), it follows that any prime divisor of $2^{2^5} + 1$ is congruent to 1 modulo $2^6 = 64$. If we wish to factor $2^{32} + 1$, it suffices to try to divide by the numbers $64k + 1$ which are primes. For $k = 1$ and $k = 6$ the number $64k + 1$ is divisible by 5 (and 385 is also divisible by 7). For $k = 2$, 5 and 8 it is divisible by 3. For 3, 4, 7, 9 and 10 the number $64k + 1$ is prime :

$$193,\ 257,\ 449,\ 577,\ 641.$$

Let us check that 641 divides $2^{32} + 1$. From $641 = 5 \cdot 2^7 + 1$ we deduce

$$5 \cdot 2^7 \equiv -1 \pmod{641},$$

hence by taking the 4th power

$$5^4 \cdot 2^{28} \equiv 1 \pmod{641}.$$

From $641 = 2^5 + 5^4$ we deduce

$$5^4 \equiv -2^4 \pmod{641}.$$

Therefore
$$1 \equiv 5^4 \cdot 2^{28} \equiv -2^4 \cdot 2^{28} \equiv -2^{32} \pmod{641}.$$
'The same proof may be given without using congruences: we use the fact that $x^4 - 1$ is divisible by $x + 1$ since
$$(x^4 - 1) = (x - 1)(x + 1)(x^2 + 1).$$
Set $x = 5 \cdot 2^7$. We deduce that $5 \cdot 2^7 + 1 = 641$ divides $5^4 \cdot 2^{28} - 1$. On the other hand $641 = 2^5 + 5^4$ divides $(2^5 + 5^4)2^{28}$. Hence 641 divides the difference
$$(2^5 + 5^4)2^{28} - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1.$$

6.
(a) Let $S = \{p_1, \dots, p_s\}$ be a finite set of primes. We first check that there exists a constant $c_1 > 0$ such that, for sufficiently large X, the number of integers m with $|m| \leq X$ of the form $m = \pm p_1^{a_1} \cdots p_s^{a_s}$ is $\leq c_1 (\log X)^s$. Indeed, for such an integer m, we have $p_i^{a_i} \leq X$, hence $a_i \leq \frac{\log X}{\log p_i}$. This proves the result with
$$c_1 = \frac{1}{(\log p_1) \cdots (\log p_s)}\cdot$$

Next, we check that there exists a constant $c_2 > 0$ such that, for sufficiently large X, the number of integers m with $|m| \leq X$ of the form $m = f(n)$ for some $n \geq 0$ in $\mathbb{Z}$, is $\geq c_2 X^{1/d}$ where d is the degree of f. Indeed, for Y a sufficiently large integer and for $0 \leq n < Y$, we have
$$|f(n)| \leq (|a_0| + \cdots + |a_d|]) Y^d$$
for $f(X) = a_0 + a_1 X + \cdots + a_d X^d$. Each of the values $f(0), f(1), \dots, f(Y-1)$ occurs at most d times. The result follows by taking $Y = c_3 X^{1/d}$ with
$$c_3 = \frac{1}{(|a_0| + \cdots + |a_d|])^{1/d}}, \qquad c_2 = \frac{c_3}{d}\cdot$$
For sufficiently large X, we have $c_2 X^{1/d} > c_1 (\log X)^s$, hence one at least of $f(n)$ with $n \in \mathbb{Z}$ is not of the form $\pm p_1^{a_1} \cdots p_s^{a_s}$. This shows that the set of primes p which divide some $f(n)$ with $n \in \mathbb{Z}$, $n \geq 0$ is infinite.
(b) For a sequence of integers $(u_n)_{n \geq 0}$, the inequality
$$\limsup_{n \to +\infty} P(u_n) < \infty$$
is equivalent to saying that the set of prime numbers which divide at least one of the u_n is finite.

References

[1] Weil, André. *Number theory for beginners,* With the collaboration of Maxwell Rosenlicht. Springer-Verlag, New York-Heidelberg, 1979. Zbl MR

[2] Hardy, G. H.; Wright, E. M. *An introduction to the theory of numbers.* Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. Zbl MR