NUMBER THEORY

CHARLES LEYTEM

Mersenne and Fermat Numbers

CONTENTS

1. The Little Fermat theorem

We start by recalling the Little Fermat theorem and a useful property.

Proposition 1.0.1. *For any prime number p and any positive integer a, $a^p - a$ is divisible by p, in other words $a^p \equiv a \pmod p$.*

Proof. We use induction on a. The property is true for $a = 1$. If it holds for a, then

$$(a+1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j \equiv a^p + 1 \equiv a + 1 \pmod p.$$

□

Corollary 1.0.2. *If p is a prime and a an integer such that $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod p$.*

Problem 1.0.3. *The sum of some given integers is 1492. Can the sum of their seventh powers be equal to 1996 (to 1998)?*

Solution. Modulo 7 the sum Σ of the integers is equal to the sum Σ_7 of their seventh powers. As 1998 is not congruent to 1492 modulo 7, Σ_7 can't be equal to 1998. Suppose the sum Σ doesn't contain terms which are larger than 3 in absolute value, i.e. it is of the form

$$\Sigma = a \cdot 1 + b \cdot (-1) + c \cdot 2 + d \cdot (-2) = (a-b) + (c-d)2.$$

Then

$$\Sigma_7 = a \cdot 1 + b \cdot (-1) + c \cdot 2^7 + d \cdot (-2)^7 = (a-b) + (c-d)2^7.$$

Solving

$$(a-b) + (c-d)2 = 1492 \qquad (a-b) + (c-d)2^7 = 1996$$

we find $a - b = 1484$ and $c - d = 4$. Thus a possible solution is $\Sigma = 1+1+\cdots+1+2+2+2+2$ with 1 occurring 1484 times.

Proposition 1.0.4. *Let a and p be integers. If $a^m \equiv 1 \pmod p$ and $a^n \equiv 1 \pmod p$ then $a^{(m,n)} \equiv 1 \pmod p$.*

Proof. We may suppose $m > n$. Write $m = nq + r$ $(0 \leq r < n)$. Then

$$1 \equiv a^m \equiv a^{nq+r} \equiv (a^n)^q a^r \equiv a^r.$$

Repeat the procedure using (n, r) instead of (m, n). Continuing this way we eventually end up with $a^{(m,n)} \equiv 1 \pmod p$. □

2. Mersenne numbers

In this section we propose some problems related to numbers of the form $2^n - 1$.

Problem 2.0.5. *Show that for even $n > 4$ the number $2^n - 1$ is the product of at least three prime numbers, two of which at least are distinct.*

Solution. We can write $n = 2k$ and $2^n - 1 = (2^k - 1)(2^k + 1)$. First note that $(2^k - 1)$ and $(2^k + 1)$ cannot have common prime factors, as they differ by 2. Thus there are at least two distinct prime factors as $n > 4$. Among the three consecutive numbers $(2^k - 1)$, 2^k, $(2^k + 1)$ one is divisible by 3, and it must be the first one or the last one. Thus $2^n - 1$ has at least three prime factors as $n > 4$.

Problem 2.0.6. *Show that $2^n - 1$ cannot be a perfect (proper) power of a prime.*

Solution. Suppose we can write $2^n - 1 = p^k$ ($k > 1$, p prime). Obviously p is odd.

Suppose k is odd. Then we have $2^n = p^k + 1 = (p+1)(p^{k-1} - p^{k-2} + \cdots + 1)$ where the second factor contains k odd terms, and thus is odd, which is impossible. Thus k must be even. Write $k = 2l$. Now

$$2^n - 1 = p^k \Leftrightarrow 2^n - 2 = p^{2l} - 1$$

Factoring out we get $2(2^{n-1} - 1) = (p^l - 1)(p^l + 1)$. As p is odd, the right hand side is divisible by 4 whereas the left hand side is only divisible by 2, a contradiction.

Problem 2.0.7. *Determine all prime numbers p such that $p \mid 2^p - 1$.*

Solution. Suppose there exists such a prime number p. Obviously p must be odd.

$$p \mid 2^p - 1 \Leftrightarrow 2^p \equiv 1 \pmod{p}.$$

By Fermat $2^{p-1} \equiv 1 \pmod{p}$. By proposition 1.0.4, $2^{(p-1,p)} \equiv 1 \pmod{p}$. As $(p-1, n) = 1$ we get $2^1 \equiv 1 \pmod{p} \Leftrightarrow p = 1$, a contradiction.

Thus there are no such primes.

Problem 2.0.8. *Determine all positive integers n such that $n \mid 2^n - 1$.*

Solution. Obviously $n = 1$ is a solution.

Suppose $n > 1$. Denote p the smallest prime in the prime decomposition of n. Obviously p is odd.

$$n \mid 2^n - 1 \Rightarrow p \mid 2^n - 1 \Leftrightarrow 2^n \equiv 1 \pmod{p}.$$

By Fermat $2^{p-1} \equiv 1 \pmod{p}$. By proposition 1.0.4, $2^{(p-1,n)} \equiv 1 \pmod{p}$. But the primes in the prime factorization of $p-1$ are smaller than those in the factorization of n. Therefore $(p-1, n) = 1$ implying $2^1 \equiv 1 \pmod{p} \Leftrightarrow p = 1$, a contradiction.

Problem 2.0.9. *Determine all positive integers $k > 1$,$n_1, n_2, \ldots, n_k$ such that*

$$n_1 \mid 2^{n_2} - 1, \quad n_2 \mid 2^{n_3} - 1, \quad \ldots \quad , n_k \mid 2^{n_1} - 1.$$

Solution. Obviously $n_1 = n_2 = \cdots = n_k = 1$ is a solution for any k. Also if one n_j equals 1 then all n_i must be 1. Let us suppose $n_i > 1$ for all i.

Denote p the smallest prime in the prime decompositions of the n_i ($i = 1, \ldots, k$). Note p is odd. Suppose p is a factor of n_j:

$$n_j \mid 2^{n_{j+1}} - 1 \Rightarrow p \mid 2^{n_{j+1}} - 1 \Leftrightarrow 2^{n_{j+1}} \equiv 1 \pmod{p}.$$

By Fermat $2^{p-1} \equiv 1 \pmod{p}$. Therefore $2^{(p-1,n_{j+1})} \equiv 1 \pmod{p}$. But the primes in the prime factorization of $p-1$ are smaller than those in the factorization of n_{j+1}. Therefore $(p-1, n_{j+1}) = 1$ implying $2^1 \equiv 1 \pmod{p} \Leftrightarrow p = 1$, a contradiction.

Problem 2.0.10. *Determine all primes p such that $\frac{2^{p-1}-1}{p}$ (the Fermat quotient of p with base 2) is a perfect square.*

Solution. Obviously $p > 2$. We have the factorization

$$2^{p-1} - 1 = (2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1).$$

Both factors are relatively prime as they are odd and differ by 2. As the prime p divides one of them, the other one has to be a square for $\frac{2^{p-1}-1}{p}$ to be a square. So depending on the case we have to solve the equation $2^x - 1 = k^2$ respectively $2^x + 1 = k^2$ with k an odd integer. We consider the two cases separately.

$2^x + 1 = k^2$.

This is equivalent to $2^x = k^2 - 1 \Leftrightarrow 2^x = (k-1)(k+1)$.

Thus $k - 1 = 2^i$ and $k + 1 = 2^j$ (i, j integer), leading to $2^j - 2^i = 2 \Leftrightarrow 2^{i-1}(2^{j-i} - 1) = 1$ with unique solution $i = 1$ and $j = 2$. We get $x = 3$ and finally $p = 7$. We check that $\frac{2^{p-1}-1}{p} = 9$, a square.

$2^x - 1 = k^2$.

If $x > 1$ it is immediate that there is no solution, as $2^x - 1 \equiv 3 \pmod 4$ and $k^2 \equiv 1 \pmod 4$. So we assume $x = 1$ and get the solution $k = 1$ leading to $p = 3$. Again we check that $\frac{2^{p-1}-1}{p} = 1$, a square.

Problem 2.0.11. *Determine all primes p such that $p^2 \mid 2^{p-1} - 1$.*

Solution. Open problem. Primes p such that $p^2 \mid 2^{p-1} - 1$ are called Wieferich primes. The only known ones are $p = 1093$ and $p = 3511$.

3. Fermat numbers

In this section we propose some problems related to numbers of the form $2^n + 1$.

Problem 3.0.12. *Show that the number $(2^{4n+2} + 1)/5$ is composite for $n > 1$ integer.*

Solution. As $2^{4n+2} = 4^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod 5$, we have $5 \mid 2^{4n+2}$. We have the factorization $2^{4n+2} + 1 = (2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1)$ and therefore 5 must divide one of the factors. For the smallest factor we have

$$2^{2n+1} - 2^{n+1} + 1 = 2^{n+1}(2^n - 1) + 1 \geq 2^3 \cdot 3 + 1 = 25$$

and it follows that $(2^{4n+2} + 1)/5$ is composite.

Problem 3.0.13. *Show that $2^n + 1$ cannot be a perfect (proper) power of a prime unless $n = 3$.*

Solution. Suppose we can write $2^n + 1 = p^k$ for p prime . Obviously p is odd.

As we have $2^n = p^k - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + 1)$ where the second factor contains k odd terms, $k = 2l$ must be even.

Then

$$2^n + 1 = p^{2l} \Leftrightarrow 2^n = p^{2l} - 1 = (p^l - 1)(p^l + 1)$$

which is only possible if $p^l - 1 = 2$ and $p^l + 1 = 4$. Therefore $p^l = 3$ and $p = 3$. Also $2^m = 2 \cdot 4$ yields $m = 3$. Therefore the unique solution is $2^3 + 1 = 3^2$.

Problem 3.0.14. *Show that for even $n > 6$ the number $2^n - 1$ is the product of at least three distinct prime numbers.*

Solution. As in problem 2.0.5 we write $n = 2k$, $2^n - 1 = (2^k - 1)(2^k + 1)$. We also recall that $(2^k - 1)$ and $(2^k + 1)$ cannot have common prime factors. Thus if $2^n - 1$ has only two distinct prime factors we must have that each factor is a prime or a perfect power of a prime. But this is impossible as 3 is a proper divisor of at least one of the factors, and by problems 2.0.6 and 3.0.13 none of the factors can be a proper perfect power of a prime.

Problem 3.0.15. *Show that that there is an infinity of positive integers n such that $n \mid 2^n + 1$.*

Solution. First solution:

We consider the integers $n = 3^k$. We proceed by induction. If $k = 1$ then then $n = 3$ and $3 \mid 2^3 + 1 = 9$. Suppose the property is true for k, i.e. $2^{3^k} + 1$ is divisible by 3^k. As we have

$$2^{3^{k+1}} + 1 = (2^{3^k} + 1)(2^{2 \cdot 3^k} - 2^{3^k} + 1)$$

we have to show that $2^{2\cdot 3^k} - 2^{3^k} + 1$ is divisible by 3. But

$$2^{2\cdot 3^k} - 2^{3^k} + 1 = 4^{3^k} - 8^{3^{k-1}} + 1 \equiv 1 + 1 + 1 \equiv 0 \pmod 3$$

Second solution:

We show that $n \mid 2^n + 1 \Rightarrow 2^n + 1 \mid 2^{2^n+1} + 1$. As $n \mid 2^n + 1$, we can write $2^n + 1 = kn$ with k odd. Therefore $2^n + 1 \mid (2^n)^k + 1 = 2^{nk} + 1 = 2^{2^n+1} + 1$.

Problem 3.0.16. *Find all prime numbers p such that $p \mid 2^p + 1$.*

Solution. The Fermat theorem implies that $p \mid 2^p - 2$. So we get $p \mid 2^p + 1 - (2^p - 2) = 3$. Therefore $p = 3$ is the only solution.

Problem 3.0.17. *Show that all positive integers $n > 1$ such that $n \mid 2^n + 1$ are of the form $n = 3^k m$ with $k \neq 0$ and m prime to 3.*

Solution Obviously n is odd. Denote p the smallest prime in the prime decomposition of n:

$$n \mid 2^n + 1 \Rightarrow p \mid 2^n + 1 \Leftrightarrow 2^n \equiv -1 \pmod p \Rightarrow 2^{2n} \equiv 1 \pmod p.$$

By Fermat $2^{p-1} \equiv 1 \pmod p$. Therefore $2^{(p-1,2n)} \equiv 1 \pmod p$. But the primes in the prime factorization of $p - 1$ are smaller than those in the factorization of n. Therefore $(p - 1, n) = 2$ implying $2^2 \equiv 1 \pmod p \Leftrightarrow p = 3$.

Problem 3.0.18. *Show that $2^{3^k} + 1$ is divisible by 3^{k+1} and not by 3^{k+2}.*

Solution. We proceed by induction. Suppose the property is true for k, i.e. $2^{3^k} + 1$ is exactly divisible by 3^{k+1}. As we have

$$2^{3^{k+1}} + 1 = (2^{3^k} + 1)(2^{3^{2k}} - 2^{3^k} + 1)$$

we have to show that $2^{3^{2k}} - 2^{3^k} + 1$ is divisible by 3 and not by 9. As

$$2^{2\cdot 3^k} - 2^{3^k} + 1 = 4^{3^k} - 8^{3^{k-1}} + 1 \equiv 1 + 1 + 1 \equiv 0 \pmod 3$$

$$2^{2\cdot 3^k} - 2^{3^k} + 1 = 8^{2\cdot 3^{k-1}} - 8^{3^{k-1}} + 1 \equiv 1 + 1 + 1 \equiv 3 \pmod 9$$

$2^{3^{2k}} - 2^{3^k} + 1$ is divisible by 3 and not by 9.

4. An IMO problem

Now we are prepared to solve:

Problem 4.0.19. *Find all positive integers n such that $\frac{2^n+1}{n^2}$ is an integer. (IMO, 1990)*

Solution. In view of problem 3.0.17 $n = 3^k m$ with m odd prime to 3. Also

$$2^n + 1 = (2^{3^k} + 1)(2^{(m-1)3^k} - 2^{(m-2)3^k} + \cdots + 1).$$

As the second factor is congruent to m modulo 3 it is not divisible by 3. Therefore by problem 3.0.18, $2^n + 1$ is divisible by exactly 3^{k+1}. But, as $2^n + 1$ divisible by n^2 it is divisible by 3^{2k} implying $2k \leq k + 1 \Leftrightarrow k = 1$. Therefor $n = 3m$.

Now let $p > 3$ be a prime dividing n.

$$n \mid 2^n + 1 \Rightarrow p \mid 2^n + 1 \Leftrightarrow 2^n \equiv -1 \pmod p \Rightarrow 2^{2n} \equiv 1 \pmod p.$$

By Fermat $2^{p-1} \equiv 1 \pmod p$. Therefore $2^{(p-1,6m)} \equiv 1 \pmod p$. But the primes in the prime factorization of $p - 1$ are smaller than those in the factorization of m. Therefore $(p - 1, 6m) =$

$1, 2, 3, 6$ implying $p = 2, 3, 4, 7$. This leaves as only possibility $p = 7$. But $2^n + 1 = 2^{3m} + 1 = 8^m + 1 \equiv 1 + 1 \equiv 2 \pmod{p}$.

Finally $n = 3$ is the only solution.

Problem 4.0.20. *Show that all Fermat numbers are square-free.*

Solution. Open problem