IDEAS FOR NEXT VERSION OF THE BOOK

ANDREW GRANVILLE

1. New question maybe: Prove that $n > 1$ never divides $2^n - 1$

Proof #1 Let n be the smallest integer such that $n|2^n-1$. Then n is odd. If 2 has order m mod n then $2^m \equiv 1 \pmod m$ and so $m = n$. But then there are n distinct reduced residues mod n, which is impossible.
Proof #2 Let p be the smallest prime dividing n so that $2^n \equiv 1 \pmod p$ and $2^{p-1} \equiv 1 \pmod p$, which implies that $2^{(n,p-1)} \equiv 1 \pmod p$. Therefore $1 < (n, p-1) \leqslant p-1 < p$, and so $(n, p-1)$, and therefore n has a prime factor smaller than p, which is impossible.

2. New appendix on Fermat's Little Theorem

Theorem 1. *For a given sequence of integers $\{a_n : n \geqslant 1\}$ define*

$$A(t) := \exp\left(\sum_{n\geqslant 1} a_n \frac{t^n}{n}\right) = 1 + \sum_{n\geqslant 1} c_n t^n.$$

The c_n are all integers if and only if

$$\sum_{m|n} \mu(\tfrac{n}{m}) a_m \equiv 0 \pmod n \text{ for all } n \geqslant 1.$$

Lemma 1. *We can write*

$$A(t) = \prod_{n\geqslant 1} (1-t^n)^{-b_n}.$$

where $c_n \in \mathbb{Z}$ for all $n \geqslant 1$ if and only if $b_n \in \mathbb{Z}$ for all $n \geqslant 1$.

Proof. We construct the sequence $\{b_N : N \geqslant 1\}$ by induction on $N \geqslant 1$, assuming that

$$\prod_{n=1}^{N-1} (1-t^n)^{-b_n} = 1 + \sum_{n=1}^{N-1} c_n t^n + c_N^* t^N + \dots,$$

so that the coefficients up to the t^{N-1} term match those of $A(t)$. This much is trivially true for $N = 1$. We expand

$$(1-t)^{-b} = 1 + bt + \sum_{k\geqslant 2} \binom{-b}{k} (-t)^k \text{ where } \binom{-b}{k} = \frac{(-b)(-b-1)\cdots(-b-(k-1))}{k!}.$$

If b is an integer then the coefficients here are all integers. By our induction hypothesis we have

$$\prod_{n=1}^{N} (1-t^n)^{-b_n} = 1 + \sum_{n=1}^{N-1} c_n t^n + (c_N^* + b_N) t^N + \dots$$

and so the coefficient can be made to equal c_N by setting $b_N = c_N - c_N^*$. The result follows, including the fact that if $c_n \in \mathbb{Z}$ if and only if $b_n \in \mathbb{Z}$ □

Proof of Theorem 1. Using Lemma 1, and taking logarithms, we have

$$\sum_{n\geqslant 1} a_n \frac{t^n}{n} = \log A(t) = -\sum_{m\geqslant 1} b_m \log(1-t^m) = \sum_{m\geqslant 1} b_m \sum_{k\geqslant 1} \frac{t^{mk}}{k} = \sum_{n\geqslant 1} \Big(\sum_{m|n} m b_m\Big)\frac{t^n}{n},$$

and so

$$a_n = \sum_{m|n} m b_m \text{ for all integers } n \geqslant 1.$$

Now, by the Möbius inversion formula we deduce that

$$b_n = \frac{1}{n}\sum_{m|n} \mu(n/m) a_m.$$

Therefore the b_n are all integers if and only if $\sum_{m|n}\mu(n/m)a_m \equiv 0 \pmod n$ for all $n \geqslant 1$, and the result follows from Lemma 1, □

Corollary 1. *Suppose that $f(x)$ is a monic polynomial with integer coefficients. We can write $f(x) = \prod_{i=1}^d (x-\alpha_i)$, and we will define*

$$f_m(x) := \prod_{i=1}^d (x-\alpha_i^m) \text{ and } s_m(f) := \prod_{i=1}^d \alpha_i^m \text{ for all } m \geqslant 1.$$

Then

$$\sum_{m|n} \mu(\tfrac{n}{m}) s_m(f) \equiv 0 \pmod n \text{ and } \sum_{m|n} \mu(\tfrac{n}{m}) f_m(x) \equiv 0 \pmod n \text{ for all } n \geqslant 1.$$

If $m = p$ is prime and $d = 1$ then $\alpha_1 \in \mathbb{Z}$ and we obtain $\alpha_1^p \equiv \alpha_1 \pmod p$, which is Fermat's Little Theorem. One can apply the Corollary with f replaced by f_ℓ for convenience. The cases of most interest are where n is a prime power since, for example, we can rewrite the case $n = pq$ with $f_{pq} - f_p - f_q + f_1 \equiv 0 \pmod{pq}$ as $((f_p)_q - (f_p)) - (f_q - f) \equiv 0 \pmod q$, and analogously mod p.

Proof. Since the α_i are all algebraic integers, therefore $s_m \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. Also

$$x^d f(1/x) = \prod_{i=1}^d (1-\alpha_i x) = \exp\Big(-\sum_{i=1}^d \sum_{n\geqslant 1} \alpha_i^n \frac{t^n}{n}\Big) = \exp\Big(\sum_{n\geqslant 1}(-s_n)\frac{t^n}{n}\Big).$$

Since the coefficients of the polynomial are all integers, starting with 1, we can apply Theorem 1 to obtain that claimed congruences for the s_m.

We observe that

$$f_m(x) = \sum_{k=0}^d (-1)^k s_m^{(k)} x^{m-k} \text{ where } s_m^{(k)} := \sum_{1\leqslant j_1<j_2<\cdots<j_k\leqslant d} (\alpha_{j_1}\cdots\alpha_{j_k})^m.$$

We now apply the first part of this proof to the polynomials

$$f^{(k)}(x) := \prod_{1\leqslant j_1<j_2<\cdots<j_k\leqslant d} (x - \alpha_{j_1}\cdots\alpha_{j_k})$$

so that $\sum_{m|n}\mu(\frac{n}{m})s_m^{(k)} \equiv 0 \pmod n$ for all $n \geqslant 1$ and so

$$\sum_{m|n}\mu(\tfrac{n}{m}) f_m(x) = \sum_{k=0}^d (-1)^k \Big(\sum_{m|n}\mu(\tfrac{n}{m}) s_m^{(k)}\Big) x^{m-k} \equiv 0 \pmod n. \qquad \square$$

3. Two new exercises, in between Exercises 8.9.10 and 8.9.11

Exercise A. Let n be a positive integer that is not a square.

(1) Use exercise 8.7.2 to show that there exists a prime p for which $(\frac{p}{n}) = -1$.
In this problem we are interested in finding odd integers b for $(\frac{n}{b}) = -1$.
(2) Show that if $n \equiv 1 \pmod 4$ then $(\frac{n}{b}) = -1$ for $b = a$ or $n - a$, selected to be odd.
(3) Show that we may assume without loss of generality that 4 does not divide n.
(4) Show that if $n \equiv 2 \pmod 4$ then $(\frac{n}{b}) = -1$ for $b = n + 1$.
(5) Show that if $n \equiv 3 \pmod 4$ then $(\frac{n}{b}) = -1$ for $b = 2n + 1$.
(6) Show that for any integer $N < 0$ there exists an integer $B > 1$ for which $(\frac{N}{B}) = -1$.
(7) Deduce that if $n \in \mathbb{Z} \setminus \mathbb{Z}^2$ then there exists a prime p for which $(\frac{n}{p}) = -1$.

Exercise B. (Another proof of Proposition 3.4.2) Assume that n is a non-square positive integer for which $\sqrt{n} = r/s \in \mathbb{Q}$ where $(r, s) = 1$.

(1) Show that if p is a prime that does not divide n then p does not divide s.
(2) Use the equation $r^2 = ns^2$ to deduce that $(\frac{n}{p}) = 0$ or 1.
(3) Now use exercise A(vi) to deduce Proposition 3.4.2.