$\mathbb{ITYM}$ 2021 - Problem 6:
Binomial Coefficients and Prime Numbers.

Team France

Composed by :

De Ridder Achille, Harter Louis-Max,
Fourcin Emile, Quille Maxime
Varnet Philémon, Leroux Hubert

Supervised by :

Lenoir Théo et Béreau Antoine

June 2021

Contents

Introduction and notations

1. $\mathbb{P}$ is the set of prime numbers.

Preliminaries

Proposition 1. Let $p \in \mathbb{P}$. For all $k \in \mathbb{N}$, we have the following polynomial congruence :

$$(X+1)^{p^k} \equiv X^{p^k} + 1 \mod p$$

Proof. We proceed by induction on k.

- Base case : for $k = 0$, $(X+1)^{p^0} \equiv (X+1)^1 \equiv X + 1 \mod p$ so it's proved.
- Inductive step : suppose the result true for $k \in \mathbb{N}$. By taking the identity exponent p, we have then

$$(X+1)^{p^{k+1}} \equiv \left(X^{p^k}+1\right)^p \equiv \sum_{i=0}^{p} \binom{p}{i} X^{ip^k} \equiv X^{p \cdot p^k} + X^{0 \cdot p^k} \equiv X^{p^{k+1}} + 1 \mod p$$

  because a well-known result is $p \mid \binom{p}{i}$ for all $i \in [\![1, p-1]\!]$. This is precisely the result for $k+1$, hence it's true for all $k \in \mathbb{N}$.

■

Theorem 2 (Lucas's Theorem)**.** Let $0 \leqslant k \leqslant n$ whose representations in base $p \in \mathbb{P}$ are $n = \sum_{i=0}^{\ell} a_i p^i$ and $k = \sum_{i=0}^{\ell} b_i p^i$. Then $\binom{n}{k} \equiv \prod_{i=0}^{\ell} \binom{a_i}{b_i} \mod p$.

Proof. Modulo p, we have the following congruences :

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} X^k &\equiv (1+X)^n \equiv (1+X)^{\sum_{i=0}^{\ell} a_i p^i} \equiv \prod_{i=0}^{\ell} (1+X)^{a_i p^i} \\
&\equiv \prod_{i=0}^{\ell} \left((1+X)^{p^i}\right)^{a_i} \equiv \prod_{i=0}^{\ell} (1+X^{p^i})^{a_i} \equiv \prod_{i=0}^{\ell} \sum_{j=0}^{a_i} \binom{a_i}{j} X^{jp^i} \\
&\equiv \sum_{r=0}^{n} \prod_{i=0}^{\ell} \binom{a_i}{b_i} X^r \mod p
\end{aligned}$$

where the second congruence of the second line comes from Theorem 1, and the last being true considering, for fixed $c \in [\![0, n]\!]$, the sum of jp^i associated to c in the expansion of the product. By identification of the coefficients the result comes immediately. ■

Questions

0.1 Integers $n \geqslant 2$ which are...

0.1.1 S-compound for $S = \{p\}$ with $p \in \mathbb{P}$

Proposition 3. Let $S = \{p\}$ with p a prime number. n is S-compound if and only if $n = p^\ell$ for some integer $\ell \geqslant 1$.

Proof. Let $n \geqslant 2$ be such S-compound integer, and $\overline{a_\ell\, a_{\ell-1}\, \ldots\, a_0}^p$ its representation in base p. if there exists $i \in [\![0, \ell-1]\!]$ such that $a_i > 0$, then by choosing $1 \leqslant k < n$ with representation in base p $\overline{a_\ell\, \ldots\, (a_i - 1)\, \ldots\, a_0}^p$, we have, by hypothesis and by Theorem 2 :

$$0 \equiv \binom{n}{k} \equiv \prod_{j=0 j\neq i}^{\ell} \binom{a_j}{a_j} \cdot \binom{a_i}{a_i - 1} = \binom{a_i}{a_i - 1} = a_i \not\equiv 0 \mod p$$

because $a_i < p$, absurd. So $a_i = 0$ for all $i \in [\![0, \ell-1]\!]$. In the same way, if $a_\ell > 1$, then with $1 \leqslant k < n$ with representation in base p $\overline{(a_\ell - 1)\, 0\, \ldots\, 0}^p$, we have

$$0 \equiv \binom{n}{k} \equiv \prod_{j=0}^{\ell-1} \binom{0}{0} \cdot \binom{a_\ell}{a_\ell - 1} = \binom{a_\ell}{a_\ell - 1} = a_\ell \not\equiv 0 \mod p$$

absurd again. So $n = \overline{1\, 0\, \ldots\, 0}^p$ which is equivalent to $n = p^\ell$. Reciprocally, if n is of this form, Theorem 2 ensures that it is well divisible by p for all $1 \leqslant k < n$, there exists $i \in [\![0, \ell-1]\!]$ such that the ith digit b_i of k is greater than n's (which is zero), so that $\binom{0}{b_i} = 0$ hence $0 = \prod_{j=0}^{\ell-1} \binom{0}{b_j} \cdot \binom{1}{0} \equiv \binom{n}{k}$ mod p. ∎

0.1.2 1-compound

The following proposition is a direct corollary from the precedent one :

Proposition 4. An integer $n \geqslant 2$ is 1-compound if and only if n is a prime power, i.e. $n = p^\ell$ for some prime number p and integer $\ell \geqslant 1$.

0.2 Around S-compoundness for infinitely many integers $n \geqslant 2$

0.2.1 Infinitely many that are S-compound

Note that compoundness is conserved by inclusion, that is if n is S-compound and $S \subseteq S'$, then n is S'-compound. In the same way, if n is ℓ-compound and $\ell' > \ell$, then n is ℓ'-compound. A direct corollary of Theorem 3 is then :

Proposition 5. Let S be a set of $\ell \geqslant 1$ prime numbers. There exist infinitely many $n \in \mathbb{N}$ such that n is S-compound.

Proof. We can just choose $p \in S$, and it's sufficient to prove the result for $S' := \{p\} \subseteq S$. But this is obvious by Theorem 3, since we can take n to be an element of $\{p^k \mid k \in \mathbb{N}\}$ which is clearly infinite. ∎

0.2.2 Infinitely many that are not S-compound

Proposition 6. Let S be a set of $\ell \geqslant 1$ prime numbers. There exist infinitely many $n \in \mathbb{N}$ such that n is not S-compound.

Proof. Let $A = \{n \in \mathbb{N} \mid \forall p \in S, p \nmid n\}$. This set is clearly infinite since it contains all natural numbers of the form $k \prod_{p \in S} p + 1$ where $k \in \mathbb{N}$ which are infinitely many. Take any $n \in A$: if n is S-compound, then in particular there exists $p \in S$ such that $p \mid \binom{n}{1} = n$, contradiction. So any $n \in A$ is not S-compound, and they are infinitely many. ∎

0.3 Around 2-compoundness when...

0.3.1 $n = p^\alpha + 1$ where $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$

Proposition 7. If $n = p^\alpha + 1$ where $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$, then n is 2-compound.

Proof. Let $n = p^\alpha + 1$ where $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$. Let q be any prime divisor of $n > 1$. We claim that n is $\{p, q\}$-compound, so 2-compound. Indeed, for all $1 < k < n-1$, we have, by Theorem 3, $p \mid \binom{p^\alpha}{k}$ and $p \mid \binom{p^\alpha}{k-1}$, so $p \mid \binom{p^\alpha}{k} + \binom{p^\alpha}{k-1} = \binom{p^\alpha + 1}{k}$. For $k \in \{1, n-1\}$, we have $q \mid \binom{n}{1} = \binom{n}{n-1} = n$. So n is $\{p, q\}$-compound, as wanted. ■

0.3.2 $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ with $p_1^{\alpha_1} < \ldots < p_s^{\alpha_s}$ and $n < q(n) + p_s^{\alpha_s}$

Proposition 8. If $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ with $p_1^{\alpha_1} < \ldots < p_s^{\alpha_s}$ and $n < q(n) + p_s^{\alpha_s}$, then n is 2-compound.

The proof of this statement, as the others, can be found in https://math.mit.edu/research/highschool/rsi/documents/2017Puig.pdf.