ARITHMETIC OF BINOMIAL COEFFICIENTS

Dmitry FUCHS

Problems

The problems below have significantly different levels of difficulty. I can predict that you will have no problems with problems 1–4 and 7. Problems 5, 6, 8, and 9(a) are more interesting, and problems 11, 12, and 13 are challenging. As to problems 9 (b), 10, and 14, I do not know their solutions, at least, elementary. I will appreciate receiving your solutions of any of the problems, especially those that are listed above as more interesting or challenging.

The notation $\binom{a}{b}$ (a choose b) means the binomial coefficient $\dfrac{a!}{b!(a-b)!}$ if $0 \le b \le a$ and 0 otherwise.

1. Prove the formulas

$$\sin m\theta = \binom{m}{1}\cos^{m-1}\theta\sin\theta - \binom{m}{3}\cos^{m-3}\theta\sin^3\theta + \binom{m}{5}\cos^{m-5}\theta\sin^5\theta - \dots$$

$$\cos m\theta = \cos^m\theta - \binom{m}{2}\cos^{m-2}\theta\sin^2\theta + \binom{m}{4}\cos^{m-4}\theta\sin^4\theta - \dots$$

$$\tan m\theta = \frac{\binom{m}{1}\tan\theta - \binom{m}{3}\tan^3\theta + \binom{m}{5}\tan^5\theta - \dots}{1 - \binom{m}{2}\tan^2\theta + \binom{m}{4}\tan^4\theta - \binom{m}{6}\tan^6\theta + \dots}$$

Below p denotes a prime number. The notation $(a_1a_2\dots a_m)_n$ means $a_1n^{m-1} + a_2n^{m-2} + \dots + a_m$. The notation $a \equiv b \bmod c$ means that $a - b$ is divisible by c.

2. (Lucas, 1878) If a, b, c, d are non-negative integers and $c < p, d < p$, then

$$\binom{pa+c}{pb+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p$$

3. (Follows from problem 2.) If $a = (a_1a_2\dots a_m)_n, b = (b_1b_2\dots b_m)_n$, then

$$\binom{a}{b} \equiv \binom{a_1}{b_1}\binom{a_2}{b_2}\dots\binom{a_m}{b_m} \bmod p$$

By the way, what percent of numbers $\binom{a}{b}$ with $0 \le b \le a \le 2^{100}$ are odd?

4. (A generalization of the criterion of divisibility by 9.) If $a = (a_1a_2\dots a_m)_n$ then $a - (a_1 + \dots + a_m)$ in divisible by $n - 1$.

5. (Related to problem 4.) Prove that the number of factors p in the prime factorization of $a!$ where $a = (a_1 \dots a_m)_p$ is $\dfrac{a - (a_1 + \dots + a_m)}{p-1}$

6. (Kummer, 1852) The number of factors p in the prime factorization of $\binom{a}{b}$ is equal to the number of "carries" when we add $a-b$ to b in the numeric system with base p.

7. (Follows from problem 6, but is easy to prove directly.) If q is not divisible by p then $\binom{p^n}{q}$ is divisible by p^n

8. (A hidden symmetry of Pascal triangle mod$p$.)If $0 \le b \le a < p$, then

$$\binom{a}{b} \equiv (-1)^{a+b} \binom{p-1-b}{p-1-a} \bmod p$$

9. (a)

$$\binom{pa}{pb} - \binom{a}{b}$$

is divisible by p^2.

(b) (Ljunggren, 1952.) If $p \ge 5$ then

$$\binom{pa}{pb} - \binom{a}{b}$$

is divisible by p^3.

10. (Greg Kuperberg, 1999.) If $\binom{2p}{p} - 2$ is divisible by p^4 then

$$\binom{pa}{pb} - \binom{a}{b}$$

is divisible by p^4 for all a, b.

Comments. According to Greg Kuperberg, the smallest prime for which the condition of problem 4 holds is 16,843. Kuperberg has a heuristic justification of a conjecture that there are infinitely many primes with this property. In 1999, he thought that the second such prime is not within the reach of today's computers. Now, he knows the second such number, but he thinks that the third such number ... (see above).

11. (Might be useful for the next problem.) If $p \ge 5$ and

$$1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{P}{Q}$$

where $\dfrac{P}{Q}$ is an irreducible fraction, then P is divisible by p^2.

12. (Albert Schwarz, 1959.) If $p \geq 5$ then $\binom{p^2}{p} - p$ is divisible by p^5 (I do not know, whether it is ever divisible by p^6).

13. (Myself, 1959.) If $n > 1$, then

$$\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$$

is divisible by 2^{2n+2}. (My solution: consider the polynomial $(1+x)^{2^{n+1}} - (1-x^2)^{2^n}$ and use problem 7.)

14. (Generalization of problem 13; mostly, Zieve, 1999.) If $p \geq 5$ then

$$\binom{ap^n}{bp^n} - \binom{ap^{n-1}}{bp^{n-1}}$$

is divisible by p^{3n}. With some minor exceptions, it is true also for $p = 2$ and 3. In particular the exponent $2n+2$ in problem 13 can be always replaced by $3n$.

Comment. I have an impression that Zieve's Theorem (problem 14) gives a more or less optimal result, although in some cases a better divisibility holds. Problem 12 gives one example; there are other strange divisibilities; for example, $\binom{18}{2b} - \binom{9}{b}$ is divisible by 2^4, and, seemingly, $\binom{34}{2b} - \binom{17}{b}$ is divisible by 2^5 for any b. Well, let us stop here.