

01/12/03

PROBLEMS ON DIVISIBILITY OF BINOMIAL COEFFICIENTS
Revised Version

Thomas J. Osler
 Mathematics Department
 Rowan University
 Glassboro, NJ 08028
Osler@rowan.edu

And

James Smoak
 12140 E. Iowa Drive
 Aurora, Co 80012
jsmoak@worldnet.att.net

1. INTRODUCTION

In this note we present several unusual problems involving divisibility of the binomial coefficients. The problems are listed in section 2. All the problems have short solutions which are listed in section 3. These problems could be assigned to students in any course in which the binomial theorem and Pascal's triangle are presented. This includes courses in precalculus mathematics, real analysis and number theory.

The following are required of the students:

1. The ability to construct Pascal's triangle and to relate the coefficients to the expansion of $(x + y)^n$.
2. The formula $C(n, r) = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}$ for the binomial coefficients is required.
3. A familiarity with prime numbers and the prime factorization of an integer.
4. *The Fundamental Theorem of Arithmetic*: Every integer greater than one can be written uniquely as a product of primes.

5. *Euclid's Lemma*: If a , b , and c are natural numbers and a divides bc , with a and b having no prime factors in common (a and b are *relatively prime*), then a divides c .

A special case of Fermat's little theorem arises naturally from the problems. This leads to the concept of pseudoprime numbers which is discussed briefly in the solutions.

2. THE PROBLEMS

In this section we list our problems on the divisibility of the binomial coefficients.

Problem 1: The fifth row, (start counting from 0th row), of Pascal's triangle is 1 5 10 10 5 1. Notice that all the numbers (except the first and last) are divisible by 5. What other rows of Pascal's triangle have the property that

$C(n,1), C(n,2), C(n,3), \dots, C(n,n-1)$ are divisible by n ?

Problem 2: Prove that $C(p,1), C(p,2), C(p,3), \dots, C(p,p-1)$ are all divisible by p when p is a prime number.

Problem 3: Prove that $aC(p,r) + bC(p,s)$ is divisible by p when p is a prime number, r and $s \in \{1, 2, 3, \dots, p-1\}$, and a and b are any integers.

Problem 4: Generalize problem 3.

Problem 5: Notice that in the following triangular segment extracted from Pascal's triangle:

$$\begin{array}{cccccc} X & 5 & 10 & 10 & 5 & X \\ X & X & 15 & 20 & 15 & X & X \\ X & X & X & 35 & 35 & X & X & X \\ X & X & X & X & 70 & X & X & X & X \end{array}$$

all the numbers are divisible by 5. By examining Pascal's triangle, find similar triangles that are divisible by 3, 7 and 11. Make a conjecture concerning these triangular arrangements of binomial coefficients.

Problem 6: Prove the following theorem.

Theorem: Let p be a given prime number. Let $n = 0, 1, 2, \dots, p-1$. Then p divides $C(p+n, r)$ when $r = n+1, n+2, \dots, p-1$.

For example, take $p=5$, then the binomial coefficients described in this theorem form the triangular segment shown in the previous problem.

Problem 7: Prove that $(a+b)^p - a^p - b^p$ is divisible by p when p is a prime number and a and b are any integers.

Problem 8: Prove that $2^{p-1} - 1$ is divisible by p whenever p is a prime greater than 2.

Problem 9: The converse of the previous problem would be: If $2^{n-1} - 1$ is divisible by n , then n is a prime number. Use a computer algebra system like Mathematica to test the validity of this converse for $n = 341$.

Problem 10: Prove that $a^p + b^p$ is divisible by p when p is a prime number and a and b are any integers such that the sum $a+b$ is divisible by p .

Problem 11: Prove that $aC(p, r)^2 + bC(p, s)^3$ is divisible by p^2 when p is a prime number, r and $s \in \{1, 2, 3, \dots, p-1\}$, and a and b are any integers.

Problem 12: Generalize problem 7.

Note:

Since the phrase “ a divides b ” occurs frequently in these problems, use of the abbreviation “ $a|b$ ” is helpful and is frequently used in books on number theory. For example, $7|21$, says “7 divides 21”. Modular arithmetic also provides another way to visualize these problems. The phrase “ a divides b ”, can also be expressed as $b \equiv 0 \pmod{a}$. For example, $21 \equiv 0 \pmod{7}$. The statement of Fermat’s little theorem (see the solution to problem 8) becomes $a^{p-1} \equiv 1 \pmod{p}$.

3. THE SOLUTIONS

The following are solutions to the problems from the previous section.

1. Rows 2, 3, 5, 7, 11, 13, 17, 19, 23, ... all have the desired divisibility property. This suggests that rows whose numbers are *prime numbers* all have this property. We will prove this in the next problem.
2. We know that $C(p, r) = \frac{p(p-1)(p-2)\cdots(p-r+1)}{r!}$. But $C(p, r)$ is an integer, so the denominator $r!$ divides the numerator. Let $a = r!$, $b = p$, and $c = (p-1)(p-2)\cdots(p-r+1)$ in our statement of Euclid's Lemma. Since $r < p$ all of the prime factors of $r!$ are less than p . Thus p and $r!$ are relatively prime and Euclid's Lemma tells us that $\frac{(p-1)(p-2)\cdots(p-r+1)}{r!} = q$ must be an integer. Therefore $C(p, r) = pq$, and we have shown that p divides $C(p, r)$.
3. Since $\frac{aC(p, r) + bC(p, s)}{p} = a\frac{C(p, r)}{p} + b\frac{C(p, s)}{p}$ and both $\frac{C(p, r)}{p}$ and $\frac{C(p, s)}{p}$ are integers by problem 2, we see at once that p divides $aC(p, r) + bC(p, s)$.
4. The sum $\sum_{r=1}^{p-1} a_r C(p, r)$ is divisible by p when p is a prime number and the a_r are any integers. The proof is a simple generalization of solution 3.
5. The theorem we conjectured is stated in problem 6.
6. The binomial coefficients specified in this theorem are the numbers in the triangular arrangements discovered in problem 5. Notice that when $n = 0$, we have the first row of this triangle and this is the same row considered in problem 2. Therefore all the numbers in this first row $C(p+0, r)$ are divisible by p . All the following rows ($n = 1$,

$2, \dots, p-1$) are constructed from previous rows using the familiar relation

$C(p+n, r) = C(p+n-1, r) + C(p+n-1, r-1)$. By problem 3, these are all divisible by p also.

7. Since $(a+b)^p - a^p - b^p = \sum_{r=1}^{p-1} C(p, r)a^{p-r}b^r$, we see that this expression is divisible by p from problem 4.

8. Since p is a prime greater than 2, we can let $a = b = 1$ in problem 7, and deduce that $2^p - 2 = 2(2^{p-1} - 1)$ is divisible by p . Since p cannot divide 2, it must divide $2^{p-1} - 1$.

Comment: This is a special case of *Fermat's little theorem* [1, p. 91] which states that $a^{p-1} - 1$ is divisible by p whenever p is prime and a is any integer which is not divisible by p .

9. The converse of problem 8 fails for the number $n = 341$. This number is composite since $341 = 11 \cdot 31$, yet 341 divides $2^{340} - 1$.

Comment: We call a composite integer n a *pseudoprime* [1, p. 94] whenever n divides $2^{n-1} - 1$. The smallest pseudoprimes are 341, 561, 645, 1105, 1387, 1729, and 1905.

There are infinitely many pseudoprimes. An interesting calculator for finding these and related numbers is found on the website [2].

10. By problem 7, the expression $\frac{(a+b)^p - a^p - b^p}{p} = q$ is an integer. Since $a+b$ is

divisible by p , $\frac{(a+b)^p}{p}$ is an integer. Therefore $\frac{a^p + b^p}{p} = \frac{(a+b)^p}{p} - q$ is an integer.

11. Since $\frac{aC(p,r)^2 + bC(p,s)^3}{p^2} = a\left(\frac{C(p,r)}{p}\right)^2 + b\left(\frac{C(p,s)}{p}\right)^2 C(p,s)$, and since both

$\frac{C(p,r)}{p}$ and $\frac{C(p,s)}{p}$ are integers by problem 2, we see that p^2 divides

$$aC(p,r)^2 + bC(p,s)^3.$$

12. The expression $\sum_{r=1}^{p-1} a_r C(p,r)^{N_r}$ is divisible by p^N where p is a prime number, the a_r

are any integers, the N_r are positive integers and N is the smallest of the powers N_r .

The proof is a simple generalization of problem 9. Further generalizations are possible involving sums of products of the binomial coefficients like

$$\sum a_r C(p,1)^{N_{r,1}} C(p,2)^{N_{r,2}} \cdots C(p,p-1)^{N_{r,p-1}}$$
 where we leave it to the reader to

complete the details.

REFERENCES

[1] Burton, David M., *Elementary Theory of Numbers*, (4th ed.), McGraw-Hill, New York, NY, 1997.

[2] Primality testing with Fermat's little theorem,

<http://www.math.fau.edu/Richman/carm.htm>.