

MAS 117

Introduction to Algebra

Assignment 6

For handing in on 28 February 2007

Write your name and student number at the top of your assignment before handing it in. Staple all the pages together. Post the assignment in the **RED** post-box on the **BASEMENT** of the Maths building before 16:00 on Wednesday.

1 (15 marks) In $\mathbb{Z}_{13}$, calculate $\frac{2}{3} + \frac{3}{5}$.

2 (20 marks) Find all solutions of the equation $x^2 = 2$ (a) in $\mathbb{Z}_{17}$; (b) in $\mathbb{Z}_{19}$.

3 (40 marks) In this question, you can define the *binomial coefficient* $\binom{n}{r}$ to be either the number of ways of subsets containing r things chosen from a set of n things, or by the formula

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

(See Probability I notes for week 4.) By convention, $0! = 1$, so $\binom{n}{0} = \binom{n}{n} = 1$.

(a) Prove that

$$\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}.$$

(b) The *Binomial Theorem* states that

$$(x+y)^n = \sum_{r=0}^n \binom{n}{r} x^r y^{n-r}.$$

Prove this, by induction or otherwise.

(c) Prove that, if p is prime and $1 \leq r \leq p-1$, then $\binom{p}{r}$ is divisible by p .

4 (25 marks) Use the Binomial Theorem (see Exercise 3) and induction on n to show that, if p is a prime number, then $n^p \equiv_p n$ for all natural numbers n . [**Hint:** Expand $(n+1)^p$ by the Binomial Theorem; all terms except the first and the last are divisible by p .]

5 Prize question A cash prize is offered for the best solution received to this question. Do not hand this in with the rest of your coursework; give your solutions to me.

(a) Let p be a prime number. Show that $a^p \equiv_p a$ for any natural number a .
Hint: Use Fermat's Little Theorem if p does not divide a . What happens when p divides a ?

(b) Show that $2^{341} \equiv_{341} 2$, but 341 is not a prime. (The number 341 is called a *pseudoprime to base 2*.)

(c) Show that $a^{561} \equiv_{561} a$ for any integer a , but 561 is not a prime. (The number 561 is called a *Carmichael number*, after Robert D. Carmichael, who first studied numbers with this property.)

Hint: Show that

- if p is prime and $m = k(p-1) + 1$, then $a^m \equiv_p a$;
- if m is a product of distinct prime numbers then $a \equiv_m b$ holds if and only if $a \equiv_p b$ for each prime number dividing m .

(d) Can you find any more Carmichael numbers?