

Department of Mathematics and Statistics,
University of Melbourne
620-351: Number Theory
Mid-Semester Test, 10 September 2008.

You may attempt all questions but only marks from the best ten questions will be counted.

*Calculators are **not** allowed.*

- (1) Find a solution to the equation $17x + 23y = 1$ in integers x and y for which x is positive.

- (2) Find *all* solutions to the congruence

$$3x \equiv 6 \pmod{15}.$$

- (3) Solve the simultaneous congruences

$$\begin{aligned}x &\equiv 3 \pmod{15} \\2x &\equiv 11 \pmod{7}.\end{aligned}$$

- (4) Calculate $3^{888} \pmod{89}$.

- (5) State, with a brief explanation, the number of solutions, modulo 77, of the congruence

$$x^2 \equiv 1 \pmod{77}.$$

You are **not** expected to solve the congruence.

- (6) Find a number n so that $\phi(n) = 216$. (You are not expected to find all such numbers.)
- (7) Explain *briefly* why, if $\phi(m) = m - 1$ then m must be prime.
- (8) Find the order of 3 modulo 35.
- (9) Decide whether 33 is a pseudoprime to base 2; show your working.
- (10) The following calculations are done with $m = 645721$ (you need not verify them);

$$\begin{aligned}m - 1 &= 8 \times 80715; & (597952)^{80715} &\equiv 54591 \pmod{m} \\(54591)^2 &\equiv 174866 \pmod{m}; & (174866)^2 &\equiv 1 \pmod{m}.\end{aligned}$$

From these calculations, can we tell

- (a) that m is prime;
- (b) that m is composite (that is, not prime);
- (c) nothing definite about whether or not m is prime?

Give a brief reason for your answer.

- (11) Show that 3 is a primitive root modulo 29; show your working.
- (12) Suppose that $p \neq q$ are (large) primes and set $m = pq$. Explain briefly why knowledge of m and of $\phi(m)$ leads *easily* to knowledge of p and q .