Hw 8

Main skills. You need to know :

- how to find inverses in Z_m.
- Fermat's little theorem
- What is an equivalence relation
- How to find equivalence classes

. Do the following problems.

1. Prove that there are infinitely many prime numbers that are congruent to 3 mod 4 .
2. Compute 2^{10^6} mod 17
3. Prove that for any integer n, $n^3 + 5n$ is divisible by 6.
4. List all invertible elements in Z_{15}.
5. Prove that the function $f Z_{100} \to Z_{100}$ defined as $f(r) = 3 \cdot r$ (where $\cdot$ is multiplication in Z_{100}) is a bijection, then find the inverse of f .
6. For each of the following relations R say whether R is an equivalence relation or not. If it is, describe its congruence classes.
   (a) R on Z^+ defined by aRb iff gcd(a, b) is odd.
   (b) R on $Z^+ - \{1\}$ defined by aRb iff gcd$(a, b) > 1$
   (c) R on Z defined by aRb iff $a + b$ is even
   (d) R on Z^+ defined by aRb iff a div b.
   (e) Let A be the set of all polynomials in one variable x with integer coefficients. R on A defined by $p(x)Rq(x)$ iff $p(x)$ and $q(x)$ have the same degree.
7. Let A be the set of all functions from Z^+ to Z^+. Let R the relation on A defined by fRg iff $f(1) = g(1)$. Prove that R is an equivalence relation. Is the set S having as elements the equivalence classes of R countable or uncountable ?
8. Prove that if p is a prime greater than 3 the equation $x^2 = 4$ has exactly 2 solutions in Z_p. How many solutions does it have in Z_{12}?