MA3H1 Topics in Number Theory
Example Sheet 2

You should attempt all the questions on this sheet. but questions Q1, Q3, Q4 will marked for credit, and must be handed in to TA Homero Gallegos Ruiz by **3pm Friday, week 4.**

(1) Solve the following system of simultaneous congruences

$$2X + 3Y \equiv 2 \pmod 5, \qquad X + 2Y \equiv 3 \pmod 5,$$
$$X + 2Y \equiv 3 \pmod 7, \qquad 4X + 3Y \equiv 4 \pmod 7.$$

(2) (a) Let $N \equiv 3 \pmod 4$ be a positive integer. Show that at least one prime factor of N is $\equiv 3 \pmod 4$.
(b) Show that there are infinitely many primes $p \equiv 3 \pmod 4$.

(3) Let $p \equiv 3 \pmod 4$ be a prime.
(a) Show that $(p-1)/2$ is odd.
(b) Show that $x^2 + 1 \not\equiv 0 \pmod p$ for all integers x. **(Hint: use Fermat's Little Theorem)**

(4) Show that there are infinitely many primes $p \equiv 1 \pmod 4$. **(Hint: suppose that $p_1, p_2, \dots, p_n$ are all the primes congruent to $1 \pmod 4$ and consider the prime factors of $N = 4(p_1 p_2 \dots p_n)^2 + 1$. You will need Q3.)**

(5) *Fermat Numbers.*
(a) Show that if $2^m + 1$ is prime then $m = 2^n$ for some n.
(b) The n-th Fermat number is $F_n = 2^{2^n} + 1$. Show that if $a \neq b$ the $\gcd(F_a, F_b) = 1$.
(c) If p is a prime and $p \mid F_n$, show that $2^{n+1} \mid (p-1)$.
(d) Deduce that for each n, there are infinitely many primes $\equiv 1 \pmod{2^n}$.
(e) The following is a famous open problem—don't try it: factor F_{12}.
(f) This is an even more famous open problem—don't try it either: show that F_n is composite for all $n \geq 5$.

(6) (a) Let p be an odd prime and x, y integers. Show that $x^2 \equiv y^2 \pmod p$ if and only if $x \equiv \pm y \pmod p$.
(b) Deduce that there are precisely $(p+1)/2$ integers u in $\{0, 1, \dots, p-1\}$ such that $u \equiv x^2 \pmod p$ for some x.
(c) Show that $x^2 + y^2 + 1 \equiv 0 \pmod p$ is soluble. **(Hint: count the integers in $\{0, 1, \dots, p-1\}$ of the form x^2 modulo p and those of the form $-1 - y^2$ modulo p.)**
(d) Show that $x^2 + y^2 + 1 \equiv 0 \pmod m$ is soluble for any squarefree odd m.