Given name:_____ **Family name:**_____

Student number:_____ **Signature:**_____

UNIVERSITY OF TORONTO
Faculty of Arts and Science

MAT 315H1S (Introduction to Number Theory)
Instructor: Yuri Burda

Midterm
February 28, 2012

Duration: 3 hours

No aids allowed

This examination paper consists of **9** pages and **5** questions. Please bring any discrepancy to the attention of an invigilator. The number in brackets at the start of each question is the number of points the question is worth.

Answer all questions.

To obtain credit, you must give arguments to support your answers.

For graders' use:

	Score
1 (15)	
2 (15)	
3 (20)	
4 (30)	
5 (20)	
Total (100)	

1. [15] Find a parametrization of all the rational solutions (x, y) of the equation

$$5x^2 - y^2 = 1$$

$x = 1, y = 2$ is a solution. Let $y - 2 = m(x - 1)$ be a line through that point. We showed that any rational solution can be obtained by intersecting this line with the curve $5x^2 - y^2 = 1$.

Plugging $y = mx + 2 - m$ we get $5x^2 - (mx + 2 - m)^2 - 1 = 0$ or

$$(5 - m^2)x^2 + ... - (2 - m)^2 - 1 = 0$$

One of the roots is $x = 1$ so the other one is $x = -\frac{(2-m)^2+1}{5-m^2}$.

Thus the required parametrization is $x = -\frac{(2-m)^2+1}{5-m^2}$, $y = -m\frac{(2-m)^2+1}{5-m^2} + 2 - m$.

2. [15]

Alice thinks of a natural number between 1 and 100 and tells that after multiplying this number by 71 she gets an answer ending in 53. What answer did Alica get?
(*hint: first find what number Alice thought of originally*)

A straightforward way of solving the question is solving the congruence $71x - 100y = 53$. This is somewhat long.

Another way: after multiplying a number by a number which is 1 mod 10 Alice gets a number which is 3 mod 10. Hence her number is 3 mod 10, i.e. of the form $10z + 3$. Now $71(10z + 3) \equiv 53 \mod 100$ or $71z + 16 \equiv 0 \mod 10$ or $z + 6 \equiv 0 \mod 10$ or $z = 4$. Thus Alice's number is 43 and the result of multiplying it by 71 is 3053

3. (a) [10] Let $x_1, \ldots, x_7$ be all the different solutions modulo 43 of the congruence $x^7 \equiv 1 \mod 43$. Find

$$x_1^5 + x_2^5 + \ldots + x_7^5 \mod 43$$

Let a be a primitive root modulo 43. Then $x_1, \ldots, x_7 \equiv 1, a^6, \ldots, a^{36} \mod 43$. Hence

$$x_1^5 + \ldots + x_7^5 \equiv 1 + a^{30} + \ldots + a^{6 \cdot 30} = \frac{(a^{30})^7 - 1}{a^{30} - 1} = \frac{(a^{42})^5 - 1}{a^{30} - 1} = 0$$

(b) [10] Find the number of solutions of the congruence

$$1 + x + x^2 + \ldots + x^{24} \equiv 0 \mod 11 \cdot 41$$

The congruence is equivalent to the system of congruences

$$1 + x + x^2 + \ldots + x^{24} \equiv 0 \mod 11; 1 + x + x^2 + \ldots + x^{24} \equiv 0 \mod 41$$

Since $(x-1)(1+x+x^2+\ldots+x^{24}) = x^{25}-1$ these congruences are equivalent to $x^{25} \equiv 1 \mod 11, x \not\equiv 1 \mod 11$ and $x^{25} \equiv 1 \mod 43, x \not\equiv 1 \mod 43$. Each of these congruences has 4 solutions, so the original congruence has 16 solutions.

4. (a) [8] Find the last three digits of 3^{400000}

$\phi(1000) = 400$ so the last 3 digits of 3^{400000} are 001 by Euler's theorem.

(b) [8] Find the last three digits of 3^{399998}

$3^{399998} = 3^{400000}/9 \equiv 1/9 \equiv 8001/9 = 889 \mod 1000$. Hence the last three digits are 889.

(c) [7] Find the last three digits of $x = 2^{400000}$

Use CRT for $1000 = 8 \cdot 125$. The number x is 0 modulo 8 and $x = 2^{400000} \equiv 1 \mod 125$, because $\phi(125) = 100$. Thus $x \equiv 1 + 125 \cdot 3 = 376 \mod 1000$

(d) [7] Find the last three digits of $2^{\left(2^{200002}\right)}$

This number is 0 mod 8. To find this number mod 125, we should first find $2^{200002} \mod \phi(125) = 100$. For this notice that this number is 0 mod 4 and 2^2 mod 25 because $\phi(25) = 20$. Thus $2^{200002} \equiv 4 \mod 100$

Hence $2^{\left(2^{200002}\right)} \equiv 2^4 = 16 \mod 125$. Since it is 0 mod 8, it is 16 mod 1000.

Hence the last three digits are 016.

5. (a) [10] Suppose that $p = \frac{3^n-1}{2}$ is a prime, where $n \geq 3$ is an integer.

   i. Show that n is odd.
   If $n = 2k$ with $k > 1$, then $\frac{3^{2k}-1}{2} = \frac{3^k-1}{2} \cdot (3^k + 1)$ is composite.

   ii. Show that $2n$ divides $p - 1$.
   Since $1 < 3^k < p$ for $1 \leq k \leq n$ and $3^n \equiv 1 \mod p = \frac{3^n-1}{2}$, the order of 3 modulo p is n. Hence $n|(p-1)$. Since n is odd and $p-1$ is even, in fact $2n|(p-1)$.

(b) [10] Suppose that 8 is a primitive root modulo a prime $p > 3$. Show that $p \equiv -1 \mod 3$.

$8 = 2^3$. Since $2^{p-1} \equiv 1 \mod p$, $p-1$ should not be divisible by 3 (otherwise $8^{\frac{p-1}{3}} \equiv 1 \mod p$; since $0 < \frac{p-1}{3} < p-1$ this contradicts the assumption that 8 is a primitive root modulo p). Thus p must be -1 modulo 3.