UNIVERSITY OF TORONTO SCARBOROUGH

MATC15 : Introduction to Number Theory

FINAL EXAMINATION

April 23, 2013

Duration – 3 hours
Aids: none

NAME (PRINT): ______________________ KEY ______________________
Last/Surname First/Given Name (and nickname)

STUDENT NO: ____

Qn. #	Value	Score
1	10	
2	10	
3	10	
4	10	
5	30	
6	30	
Total	100	

TOTAL: ____________

Please read the following statement and sign below:

I understand that any breach of academic integrity is a violation of The Code of Behaviour on Academic Matters. By signing below, I pledge to abide by the Code.

SIGNATURE:________________________________

(1) For the problem below, you may use (without proof) that 1307 is prime.

(a) (5 points) Determine the value of the Legendre symbol $\left(\frac{5}{1307}\right)$.

By Quadratic Reciprocity, we have

$$\left(\frac{5}{1307}\right)\left(\frac{1307}{5}\right) = (-1)^{2\cdot\frac{1307-1}{2}} = 1 \tag{*}$$

Now, $\left(\frac{1307}{5}\right) = \left(\frac{2}{5}\right)$. By Euler's Criterion, we have

$$\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}} \pmod 5 \equiv 4 \pmod 5,$$

from which we deduce that $\left(\frac{2}{5}\right) = -1$. Plugging this into (*) yields

$$\left(\frac{5}{1307}\right) = -1.$$

(b) (5 points) Find all $x \in \mathbb{Z}$ such that $1307 \mid x^2 - 5$.

By part (a), 5 is a quadratic non-residue $\pmod{1307}$, i.e.

$$x^2 \not\equiv 5 \pmod{1307}$$

for all x. It follows that $1307 \nmid x^2 - 5$ for all $x \in \mathbb{Z}$. So, there are no solutions.

continued on page 3

(2) (a) (5 points) Use the Euclidean algorithm to determine $(37, 50)$.

We have

$$\begin{aligned} 50 &= 1 \times 37 + 13 \\ 37 &= 2 \times 13 + 11 \\ 13 &= 1 \times 11 + 2 \\ 11 &= 5 \times 2 + 1 \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Thus, $(37, 50) = 1$.

(b) (5 points) Solve the equation $37x = 3$ in $\mathbb{Z}_{50}^{\times}$. (You must show work to receive credit!)

Since $(37, 50) = 1$, we see that $37 \in \mathbb{Z}_{50}^{\times}$. Thus, we can divide both sides by 37:

$$x = 37^{-1} \cdot 3.$$

Thus we just have to determine 37^{-1} in $\mathbb{Z}_{50}^{\times}$.

From part (a) we have

$$\begin{aligned} 1 &= 11 - 5 \times 2 \\ &= 11 - 5 \times (13 - 1 \times 11) \\ &= -5 \times 13 + 6 \times 11 \\ &= -5 \times 13 + 6 \times (37 - 2 \times 13) \\ &= 6 \times 37 - 17 \times 13 \\ &= 6 \times 37 - 17 \times (50 - 37) \\ &= 23 \times 37 - 17 \times 50 \end{aligned}$$

It immediately follows that $23 \times 37 = 1$ in $\mathbb{Z}_{50}^{\times}$, i.e. $37^{-1} = 23$. Thus, the unique solution to our equation is

$$x = 37^{-1} \cdot 3 = 19.$$

continued on page 4

(3) (a) (2 points) List all elements of $\mathbb{Z}_{10}^{\times}$.

$1, 3, 7, 9$

(b) (3 points) Write down the multiplication table for $\mathbb{Z}_{10}^{\times}$.

$\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(c) (3 points) Determine the order of each element of $\mathbb{Z}_{10}^{\times}$.

If $\ell_a(n)$ denotes the order of $a \pmod n$, then $\ell_1(10) = 1$ (because $1^1 = 1$), $\ell_3(10) = 4$ (because $3^4 = 1$ and $3^k \neq 1$ for $k < 4$), $\ell_7(10) = 4$ (because $7^4 = 1$ and $7^k \neq 1$ for $k < 4$), and $\ell_9(10) = 2$ (because $9^2 = 1$ but $9^1 \neq 1$).

(d) (2 points) Find all primitive roots of $\mathbb{Z}_{10}^{\times}$.

Recall that $a \in \mathbb{Z}_n^{\times}$ is a primitive root iff it order is $\varphi(n)$ (equivalently, if a generates all of $\mathbb{Z}_n^{\times}$). Since $\varphi(10) = 4$, we see by part (c) that 3 and 7 are both primitive roots of $\mathbb{Z}_{10}^{\times}$, while 1 and 9 are not.

continued on page 5

(4) (10 points) Prove that there exists a prime between n and n^2 for all sufficiently large n. (You may use, without proof, any theorems proved in class.)

By Chebyshev's theorem, there exist positive constants a and b such that

$$\frac{ax}{\log x} \leq \pi(x) \leq \frac{bx}{\log x}$$

for all sufficiently large x. Thus, for all sufficiently large n, the number of primes between n and n^2 is

$$\begin{aligned}
\pi(n^2) - \pi(n) &\geq \frac{an^2}{\log(n^2)} - \frac{bn}{\log n} \\
&= \frac{an^2 - 2bn}{2\log n} \\
&\geq \frac{an - 2b}{2} \qquad \text{since } \log n \leq n \text{ for all } n \geq 1 \\
&\geq 1
\end{aligned}$$

so long as $n \geq \frac{2b+2}{a}$.

[To see that $\log x \leq x$ for all $x \geq 1$, observe that

$$\log x = \int_1^x \frac{dt}{t} \leq \int_1^x dt = x - 1 \leq x$$

for all $x \geq 1$.]

We conclude that for all sufficiently large n, there is at least one prime between n and n^2.

continued on page 6

(5) (30 points) State and prove the Law of Quadratic Reciprocity.

See lecture summaries.

continued on page 7

(6) (30 points) Prove that $\mathbb{Z}_p^\times$ has a primitive root for all primes p.

See lecture summaries.

Total Marks = 100 points