MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 2

Trinity College Dublin

Course homepage

Answers are due for Friday October 17th, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Cracking the code (100pts)*

In this exercise, we will see how an extremely common encryption algorithm (RSA encryption) functions, by reverse engineering my favourite three digit number n, and getting a bit of practice with computing totient functions

i) (10 pts) Compute $\phi(2025)$.

My favourite three digit number n satisfies

$$n^{17} \equiv 1674 \pmod{2491}$$

You, as experts at arithmetic, know that $2491 = 47 \times 53$. This will be my undoing.

ii) (10 pts) Determine $(n^{17} \pmod{47})$ and $(n^{17} \pmod{53})$

iii) (15pts) Determine the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/46\mathbb{Z}$

iv) (20 pts) Hence determine ($n \pmod{47}$)

v) (15 pts) Determine the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/52\mathbb{Z}$

vi) (15 pts) Hence determine ($n \pmod{53}$)

vii) (15 pts) Use the Chinese remainder theorem, determine $n \pmod{2491}$ and hence uncover my favourite three digit number n.

Hint: Recall that $k^a \equiv k^b \pmod{n}$ if $a \equiv b \pmod{\phi(n)}$. You may also use, without proof, that 47 and 53 are prime, and that

$$8(53) - 9(47) = 1$$

You may also use, without proof, that

$$31^{48} \equiv 13 \pmod{53}$$

though this in unnecessary if you are willing to compute an extra inverse.

This was the only exercise that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Practice with arithmetic and inverses*

Evaluate the following modular arithmetic expressions, giving your answer as a non-negative number less than the modulus.

i) $(\overline{33})(\overline{6}) - \overline{8}$ in $\mathbb{Z}/9\mathbb{Z}$,

ii) $\overline{12} + (\overline{-2})(\overline{5})$ in $\mathbb{Z}/13\mathbb{Z}$,

iii) $\overline{729}^{729}$ in $\mathbb{Z}/8\mathbb{Z}$,

iv) $\overline{47}^{-1}$ in $\mathbb{Z}/111\mathbb{Z}$,

v) $\overline{33}^{-1}$ in $\mathbb{Z}/252\mathbb{Z}$.

Exercise 3 *Tricks for surviving the cube* ★

For $n \in \mathbb{N}$, prove the following:

i) $3|n$ if and only if 3 divides the sum of the digits of n,

ii) $9|n$ if and only if 9 divides the sum of the digits of n,

iii) $11|n$ if and only if 11 divides the alternating sum of the digits of n

For example 11 *does not divide* 252 *as* 11 *does not divide* $2-5+2=-1$.

iv) $7|n$ if and only if 7 divides the difference of the last 3 digits and the number given by the remaining digits

For example, 7 *divides* 71092 *since* 7 *divides* $71-(092)=-21$.

Exercise 4 *Chinese remainder practice* ★

Find a solution in $\mathbb{Z}/456\mathbb{Z}$ to the simultaneous congruences

$$\begin{cases} x \equiv 57 \pmod 8 \\ x \equiv 8 \pmod{57} \end{cases}.$$

Exercise 5 *More divisibility*

i) Prove that $120|(n^5 - 5n^3 + 4n)$ for every $n \in \mathbb{N}$,

ii) Determine the remainder on division by 8 of

$$1! + 2! + \cdots + 60!,$$

iii) Let p be prime and

$$\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{p-1}$$

be such that $\gcd(a, b) = 1$. Show that $p|a$

Hint: Note that $p \nmid b$, and argue that

$$\overline{a}\overline{b}^{-1} = \overline{1} + \overline{2}^{-1} + \cdots + \overline{p-1}^{-1}$$

in $\mathbb{Z}/p\mathbb{Z}$, and not that inversion is a bijection.

Exercise 6 *Digit sums* ★

Let $A = 4444^{4444}$ and let B be the sum of digits of A. Let C be the sum of digits of B and let D be the sum of digits of C.

i) Determine $D \pmod 9$.

ii) Prove that $D \leq 14$

Hint: 4444^{4444} has at most $20,000$ digits. How many could B have?

iii) Determine D.

Exercise 7 *Inverse Euler*

i) Using an explicit formula for $\phi(n)$, show that if $p^k|n$, then $(p-1)p^{k-1}|\phi(n)$ for any $k \geq 1$.

ii) Hence show that if $\phi(n) = 4$, n is not divisible by any prime $p \geq 7$.

iii) Hence determine all n such that $\phi(n) = 4$.

iv) Determine all n such that $\phi(n)$ is odd.

Hint: What primes can n be divisible by?

Exercise 8 *Infinite primes* ★

The goal of this exercise is to show that there are infinitely many primes of the form $6k - 1$.

i) Show that if p is prime and $p > 3$, then $p \equiv \pm 1 \pmod 6$.

ii) By considering a number of the form $N = 6p_1p_2 \dots p_k - 1$ for distinct primes $p_1, \dots, p_k \equiv -1 \pmod 6$, show that there are infinitely many such primes.

Hint: What must the prime factors of N look like if there are only finitely many $p \equiv -1 \pmod 6$?

iii) Where does this proof fail for primes of the form $6k + 1$?

iv) Dirichlet's theorem on primes in arithmetic progression says that for any coprime $a, b \in \mathbb{Z}$, there are infinitely many primes of the form $ak + b$ for $k \in \mathbb{Z}$. Why must we have $\gcd(a, b) = 1$?

Exercise 9 *Non-solutions*

Show that the following Diophantine equations have no solutions, or prove me wrong:

i) $x^3 + y^3 = 300$,

ii) $x^2 + 12y^2 + z^2 = 319$,

iii) $x^3 + 8y^3 - 18z^2 = 48$

iv) $x^2 + 6xy + y^2 = 42$

Exercise 10 *Finding primitive roots*

i) What percentage of elements of $(\mathbb{Z}/43\mathbb{Z})^\times$ are primitive roots?

ii) Find a primitive root $\overline{g}$ of $(\mathbb{Z}/43\mathbb{Z})^\times$

iii) Determine the multiplicative order of $\overline{g}^{2024}$

iv) For which integers m is $\overline{g}^m$ another primitive root? Give a complete set of primitive roots.

Exercise 11 *Advanced divisibility*

i) Prove that $2^{3n+5} + 3^{n+1}$ is divisible by 5 for all $n \in \mathbb{N}$,

Hint: Find the multiplicative orders of the two terms

ii) Prove that $n^2 + 3n + 5$ is never divisible by 121 for any $n \in \mathbb{N}$.

Hint: Start by considering this expression modulo 11*, and use this to narrow down possible* n *for which it could be divisible by* 121*.*

Exercise 12 *Some very big remainders*

The goal of this problem is to compute some very large remainders, and practice computing the totient function. Part 1) will be useless for the rest.

i) Compute $\phi(2024)$.

ii) Determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 17.

iii) Determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 19.

iv) By using the Chinese Remainder Theorem, determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 323.

Hint: Recall that $k^a \equiv k^b \ (mod\ n)$ *if* $a \equiv b \ (mod\ \phi(n))$*. You may also use without proof that* $9(17) - 8(19) = 1$*.*

Exercise 13 *Hensel's lemma*

The goal of this exercise is to prove a result called Hensel's lemma, which gives a criterion for a polynomial to have solutions modulo p^k for every $k \geq 1$, without giving an example of this solution, where p is any prime number.

First define a linear map on $D : \mathbb{Z}[x] \to \mathbb{Z}[x]$ on the space of polynomials with integer coefficients given by

$$D(x^n) = nx^{n-1}$$

for every $n \geq 0$. We call this the formal derivative map. Note that D also defines a map on the space of polynomials with $\mathbb{Z}/N\mathbb{Z}$ coefficients by the same formula.

i) Show that, for any $a \in \mathbb{Z}$ and any $n, k \in \mathbb{N}$,

$$(x + ap^k)^n \equiv x^n + nap^k x^{n-1} \pmod{p^{k+1}}.$$

Hint: Apply the binomial theorem.

ii) Hence conclude that, for any polynomial $f \in \mathbb{Z}[x]$, we have that

$$f(x + ap^k) \equiv f(x) + ap^k (Df)(x) \pmod{p^{k+1}}.$$

iii) Suppose we have an $m \in \mathbb{Z}$ such that

$$f(m) \equiv 0 \pmod{p^k}, \quad \text{and} \quad (Df)(m) \not\equiv 0 \pmod{p}.$$

Prove that we can find $0 \leq a < p$ such that

$$f(m + ap^k) \equiv 0 \pmod{p^{k+1}}.$$

Hint: Note that for $cp^k \equiv 0 \pmod{p^{k+1}}$, it is sufficient to have $c \equiv 0 \pmod{p}$.

iv) Hence conclude that if there exists $m \in \mathbb{Z}$ such that

$$f(m) \equiv 0 \pmod{p} \quad \text{and} \quad (Df)(m) \not\equiv 0 \pmod{p},$$

then there exists $m_k \in \mathbb{Z}$ such that $f(m_k) \equiv 0 \pmod{p^k}$ for every $k \in \mathbb{N}$.

v) Explain why this is not sufficient for f to have an integer solution, and give an example of such an f.