MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 2

Trinity College Dublin

Course homepage

Answers are due for Friday October 11th, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Some very big remainders (100pt)*

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.

1. (10 pts) Compute $\phi(2024)$.
2. (30 pts) Determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 17.
3. (30 pts) Determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 19.
4. (30 pts) By using the Chinese Remainder Theorem, determine the remainder of $11^{\left(27^{2024}\right)}$ on division by 323.

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

Solution 1

1. We first find all prime factors of 2024. From our divisibility tricks, this is divisble by 8: $2024 = 8(253)$. Checking what primes divide 253, we find $253 = 11(23)$, both of which are prime. Hence

$$\phi(2024) = 2024\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{23}\right) = 880.$$

2. From Fermat's Little Theorem, we know that

$$27^{16} \equiv 1 \pmod{17}$$

Indeed, as the hint states, $27^a \pmod{17}$ depends only on the equivalence class of $a \pmod{16}$. Euler's theorem gives us that

$$a^8 = a^{\phi(16)} \equiv 1 \pmod{16}.$$

As $8|2024$, we therefore have that

$$27^{2024} \equiv 1 \pmod{16}$$

and so

$$11^{27^{2024}} \equiv 11^1 \equiv 11 \pmod{17}.$$

Then, as $0 \leq 11 < 17$, we must have that 11 is the remainder upon division by 17.

3. The same arguments apply here. We note that $\phi(19) = 18$ and $\phi(18) = 6$. As $2024 \equiv 2 \pmod{6}$, we must have that

$$27^{2024} \equiv 9^2 \equiv 81 \equiv 9 \pmod{18}$$

and hence

$$11^{27^{2024}} \equiv 11^9 \pmod{19}$$

Now

$$11^3 \equiv 1 \pmod{19}$$

so

$$11^{27^{2024}} \equiv 1^3 \equiv 1 \pmod{19}.$$

Thus, the remainder on division by 19 is 1.

4. Note that $323 = 17 \times 19$ and hence the remainder on division by 323 will be the unique $0 \leq r < 323$ such that
$$\begin{cases} r \equiv 11 \pmod{17} \\ r \equiv 1 \pmod{19} \end{cases}$$
By the explicit bijection given in the Chinese remainder theorem, this r satisfies
$$r \equiv 9(17) - 11(8)(19) \equiv -1519 \equiv 96 \pmod{323}.$$
Hence, the remainder on division by 323 is 96.

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 $\mathbb{Z}/252\mathbb{Z}$.

Solution 2

i) Note that $3|33$ and $3|6$, so $9|(33 \times 6)$, so the first term vanishes. Then $\overline{-8} = \overline{1}$ in $\mathbb{Z}/9\mathbb{Z}$.

ii) $\overline{12} + \overline{-10} = \overline{2}$ in $\mathbb{Z}/13\mathbb{Z}$.

iii) Note that $729 = 91(8)+1$, so $\overline{729} = \overline{1}$ in $\mathbb{Z}/8\mathbb{Z}$, and so $\overline{729}^{729} = \overline{1}^{729} = \overline{1}$.

iv) We need to compute the multiplicative inverse of $\overline{47}$, and we do so via Euclid's algorithm

$$\begin{aligned} 111 &= 2(47) + 17 \\ 47 &= 2(17) + 13 \\ 17 &= 13 + 4 \\ 13 &= 3(4) + 1, \end{aligned}$$

which gives us that

$$26(47) - 11(111) = 1$$

and hence $\overline{47}^{-1} = \overline{26}$ in $\mathbb{Z}/111\mathbb{Z}$.

v) Trick question! $\overline{33}$ is not invertible here, as $\gcd(33, 252) = 3 \neq 1$.

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* $71 - (092) = -21$.

Solution 3

i) We can write n in terms of its digits via

$$n = n_0 + 10n_1 + 100n_2 + 1000n_3 + \cdots 10^k n_k$$

where n is the number of digits of n. Note that $10^k \equiv 1 \pmod 3$ for every $k \geq 0$. Thus

$$n \equiv n_0 + n_1 + \cdots + n_k \pmod 3$$

from which the claim follows.

ii) A similar argument holds, as $10^k \equiv 1 \pmod 9$.

iii) Note that $10^k \equiv (-1)^k \pmod{11}$. Thus

$$n \equiv n_0 - n_1 + n_2 - \cdots \pm n_k \pmod{11}$$

from which the claim follows.

iv) Note that $1000 \equiv -1 \pmod 7$. So, letting A be the last 3 digits of n and B be the number formed by the remaining digits, we have that

$$n \equiv 1000B + A equiv A - B \pmod 7$$

from which the claim follows.

Exercise 4 *Chinese remainder practice* ★

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

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

Solution 4

We first note that 8 and 57 are coprime, and so a solution exists. We will also simplify the system to

$$\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 8 \pmod{57} \end{cases}.$$

We now present two constructions of a solution. The first uses the bijection from the proof of the Chinese remainder theorem. We note that

$$1 = 57 - 7(8)$$

and hence

$$x \equiv 8 \times (-7) \times 8 + 57 \equiv 8 + 57 \equiv 65 \pmod{456}$$

is the solution.

Alternatively, we note that if $x \equiv 8 \pmod{57}$, then there exists $k \in \mathbb{Z}$ such that $x = 57k + 8$. Substituting this into the second congruence gives

$$x \equiv 57k + 8 \equiv k \equiv 1 \pmod{8}$$

and so there exists $\ell \in \mathbb{Z}$ such that $k = 8\ell + 1$, and so $x = 57(8\ell + 1) + 8 = 456\ell + 65$. Thus $x \equiv 65 \pmod{456}$ is the solution.

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.

Solution 5

i) Let $f(n) = n^5 - 5n^3 + 4n$. It suffices to show that $3|f(n)$ and $4|f(n)$ and $5|f(n)$ as $120 = 3 \times 4 \times 5$ and these are pairwise coprime. Also note that $f(n) \pmod 3$ will have period 3, etc, so we just need to check that these statements hold for $n = 0, 1, 2, 3, 4$.

$$f(0) = f(1) = f(2) = 0,\ f(3) = 120\, f(4) = 720$$

all of which are clearly divisible by 3,4, and 5.

ii) Note that $(4!)|(n!)$ for every $n \geq 4$ and $8|(4!) = 24$. Hence $n! \equiv 0 \pmod 8$ for every $n \geq 4$. Thus

$$1! + 2! + \cdots + 60! \equiv 1 + 2 + 6 \equiv 1 \pmod 8,$$

so the remainder is 1 on division by 8.

iii) First note that, by taking a common denominator, we must have that $b|(p-1)!$ and hence $gcd(b,p)|gcd((p-1)!, p) = 1$. Thus, b is invertible in $\mathbb{Z}/p\mathbb{Z}$. Rearranging

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

we get that

$$a \prod_{k=1}^{p-1} k = b \left(\sum_{k=1}^{p-1} \prod_{\substack{1 \leq \ell \leq p-1 \\ \ell \neq k}} k \right)$$

which is an integer equation and can be reduced modulo p. Multiplying both sides of the reduced equation by

$$\overline{b}^{-1} \prod_{k=1} \overline{k}^{-1}$$

we get that the reduced equation is equivalent to

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

Since the map $\overline{k} \mapsto \overline{k}^{-1}$ is a bijection, the right hand side is just a permuted version of

$$\overline{1} + \overline{2} + \cdots + \overline{p-1}$$

which is equal to

$$\overline{\frac{p(p-1)}{2}} = \overline{0}.$$

and so $\overline{a}\overline{b}^{-1} = \overline{0}$. Multiplying both sides by $\overline{b}$ shows that $p|a$.

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.

Solution 6

i) From Exercise 3, we know that A is congruent to its digit sum modulo 9, and so $A \equiv B \pmod 9$. Similarly $B \equiv C$ and $C \equiv D$ so

$$D \equiv A \equiv 4444^{4444} \equiv (4+4+4+4)^{4444} \equiv 7^{4444} \pmod 9.$$

Then, noting that $7^3 \equiv 1 \pmod 9$ and that $4444 = 3(1481)+1$, we find that

$$D \equiv 7^{4444} \equiv 7 \pmod 9.$$

ii) If A has at most $20,000$ digits, then

$$B \leq 9(20,000) < 200,000.$$

The number with the largest digit sum in this range is $199,999$ and hence we have that

$$C \leq 1+9+9+9+9+9 = 46.$$

The number with the largest digit sum in this range is 39 and so

$$D \leq 3+9 = 14.$$

iii) There is exactly one number between 0 and 14 which is congruent to 7 (mod 9), which is 7. Thus $D = 7$.

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?

Solution 7

i) We recall that

$$\phi(n) = \prod_{p|n} p^{v_p(n)-1}(p-1).$$

If $p^k|n$, then $k \leq v_p(n)$, and so $p^{k-1}(p-1)$ divides the factor $p^{v_p(n)-1}(p-1)$ and hence $\phi(n)$.

ii) If $p|n$, then $(p-1)|\phi(n)$. So if $\phi(n) = 4$, $p - 1 \leq 5$ and so $p \leq 5$. In particular, if $\phi(n) = 4$, no prime $p \geq 7$ divides n.

iii) Thus, if $\phi(n) = 4$, $n = 2^a \times 3^b \times 5^c$. Noting that if $b > 1$, then $3|\phi(n) = 4$ and if $c > 1$ then $5|\phi(n) = 4$, we conclude that $b, c \leq 1$. Similarly, if $a \geq 4$, then $8|\phi(n) = 4$, so we must have $a \leq 3$. Running through all possible options, the only n for which we have $\phi(n) = 4$ are

$$\{5, 8, 10, 12\}.$$

iv) Note that $(p-1)$ is even for every odd prime, and so $\phi(n)$ is even if n is divisible by an odd prime. Thus $\phi(n)$ is odd only for $n = 2^a$. From our explicit formula, we in fact have that $\phi(n)$ is odd only for $a \leq 1$. Thus $n = 1$ and $n = 2$ are the only natural numbers for which $\phi(n)$ is odd.

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 $N = 6p_1p_2 \dots p_k$ 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 $\gcd(a, b) = 1$?

Solution 8

i) If $p \pmod 6 \in \{0, 2, 4\}$, then $p \in \{6k, 6k+2, 6k+4\}$ for some $k \in \mathbb{Z}$, all of which are divisible by 2. Similarly if $p \equiv 3 \pmod 6$, then $p = 6k + 3$ for some k and so $3|p$. Thus, if p is prime, it must be equivalent to 1 or $5 \equiv -1$ modulo 6.

ii) Suppose we have finitely many such primes $p_1, \dots, p_k$ congruent to -1 modulo 6, and consider $N = 6p_1 \dots p_k - 1$. This is coprime to every prime in the list $2, 3, p_1, \dots, p_k$, and so must have only prime factors $q_1, \dots, q_r \equiv 1 \pmod 6$. But then

$$N = q_1^{a_1} q_2^{a_2} \dots q_r^{a_r} \equiv 1^{a_1} \times 1^{a_2} \times \dots \times 1^{a_r} \equiv 1 \pmod 6$$

despite the fact that

$$N = 6p_1 \dots p_k - 1 \equiv -1 \pmod 6.$$

This gives a contradiction, and so there must exist another prime congruent to -1 modulo 6, and hence infinitely many such primes.

iii) For primes of the form $6k+1$, the same argument works up until the point where we conclude that all the prime factors of N must be congruent to $-1 \pmod 6$. In the next line, we then conclude

$$N \equiv (-1)^{a_1 + \dots + a_r} \pmod 6$$

which cannot always contract $N \equiv -1 \pmod 6$.

iv) If $d|a$ and $d|b$, then $d|(ak+b)$ for every k and so $ak+b$ is never prime if $d > 1$.

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

Solution 9

i) Consider this modulo 9. Cubes modulo 9 take values 0,1 or -1, so

$$x^3 + y^3 \pmod 9 \in \{0, \pm 1, \pm 2\}$$

but $300 \equiv 3 \pmod 9$, so there can be no solutions.

ii) Consider this modulo 4. We obtain the congruence

$$x^2 + z^2 \equiv 3$$

but the left hand side can only take values $\{0, 1, 2\} \pmod 4$. Therefore, there are no integer solution.

iii) Consider this modulo 9. We obtain the congruence

$$x^3 - y^3 \equiv 3 \pmod 9$$

but the left hand side only takes values $\{0, \pm 1, \pm 2\} \pmod 9$, so there can be no integer solutions.

iv) Consider this modulo 4. We obtain the congruence

$$x^2 + 2xy + y^2 \equiv 2 \pmod 4.$$

We could check all possible combinations of x and y, or we could note that the left hand side is $(x+y)^2$, which can only take values in $\{0, 1\}$ $\pmod 4$, and hence no integer solutions can exist.

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.

Solution 10

1. Since 43 is prime, $(\mathbb{Z}/43\mathbb{Z})^\times$ has a primitive root and therefore has exactly $\phi(\phi(43)) = \phi(42)$ primitive roots. We can easily check that $\phi(42) = 42(\frac{1}{2})(\frac{2}{3})(\frac{6}{7}) = 12$, and so $12/42 \approx 28.6\%$ of the elements are primitive roots.

2. Since $42 = 2 \times 3 \times 7$, we need to find $\overline{g}$ such that $\overline{g}^6$, $\overline{g}^{14}$ and $\overline{g}^{21}$ are all not $\overline{1}$.

   Lets try $\overline{g} = \overline{2}$. We have that $\overline{2}^6 = \overline{64} = \overline{21} \neq \overline{1}$, but
   $$\overline{2}^{14} = \overline{4}^7 = \overline{21}^2 \times \overline{4} = \overline{21} \times \overline{-2} = \overline{-42} = \overline{1}.$$

   In contrast
   $$\overline{3}^6 = \overline{81} \cdot \overline{9} = \overline{-5} \cdot \overline{9} = \overline{-45} = \overline{-2} \neq \overline{1}$$
   $$\overline{3}^14 = \overline{3}^12 \cdot \overline{9} = \overline{-2}^2\overline{9} = \overline{36} = \overline{-7} \neq \overline{1}$$
   $$\overline{3}^{21} * = \overline{3}^14 \cdot \overline{3}^6 \cdot \overline{3} = \overline{-7} \cdot \overline{-23} = \overline{-1} \neq \overline{1}$$

   and so $\overline{g} = \overline{3}$ is primitive!

3. We have a neat little formula which says that
   $$MO(\overline{k}^m) = \frac{MO(\overline{k})}{\gcd(MO(\overline{k}, m)}.$$

   In our case $MO(\overline{g} = 42$, and $\gcd(42, 2024) = 2$, so
   $$MO(\overline{g}^{2024}) = 1012.$$

4. $\overline{g}^m$ is primitive if and only if it has multiplicative order 42, which occurs if and only if $\gcd(m, 42) = 1$. Thus the primitive roots are
   $$\{\overline{3}^m \mid m = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}.$$

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*.*

Solution 11

i) Note that 2^{3n+5} has multiplicative order at most 4. Checking quickly, we see that 2^{3n+5} defines a periodic sequence in $\mathbb{Z}/5\mathbb{Z}$ given by

$$\{\overline{1}, \overline{3}, \overline{4}, \overline{2}, \overline{1}, \ldots\}.$$

Similarly, 3^{n+1} defines a periodic sequence in $\mathbb{Z}/5\mathbb{Z}$ given by

$$\{\overline{4}, \overline{2}, \overline{1}, \overline{3}, \overline{4}, \ldots\}.$$

As both sequences have period 4, it suffices to check that $2^{3n+5} + 3^{n+1}$ is divisible by 5 just for the first 4 terms, and indeed we see that we get

$$\{\overline{1} + \overline{4} = \overline{0}, \overline{3} + \overline{2} = \overline{0}, \overline{4} + \overline{1} + \overline{0}, \overline{2} + \overline{3} = \overline{0}\}$$

in $\mathbb{Z}/5\mathbb{Z}$. Hence $5 | 2^{3n+5} + 3^{n+1}$ for all $n \geq 1$.

ii) We start by considering $f(n) = n^2 + 3n + 5 \pmod{11}$. Running through $n \equiv 0, 1, \ldots, 10 \pmod{11}$, we find that $f(4) \equiv 0 \pmod{11}$, but is non-zero for all other congruence classes. Hence if $121 | f(n)$ (which implies that $11 | f(n)$) for some $n \in \mathbb{Z}$, $n \equiv 4 \pmod{11}$. Let $n = 11k + 4$. Then

$$f(11k + 4) = 121k^2 + 88k + 16 + 33k + 12 + 5 = 121k^2 + 121k + 33$$

which can never be divisible by 121, as $121 | (121k^2 + 121k)$, but $121 \nmid 33$.

Exercise 12 *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.

Solution 12

i) Via the binomial theorem

$$\begin{aligned}(x+ap^k)^n &= x^n + nap^k x^{n-1} + \sum_{i=2}^{n} \binom{n}{i} (ap^k)^i x^{n-i} \\ &= x^n + nap^k x^{n-1} + p^{2k} \sum_{i=2}^{n} \binom{n}{i} a^i p^{ki-2k} x^{n-i} \\ &\equiv x^n + nap^k x^{n-1} \pmod{p^{k+1}}\end{aligned}$$

for all $k \geq 1$.

ii) The above statement can be rewritten as

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

Since $f(x+ap^k)$ is an integer linear combination of monomials $(x+ap^k)^n$, the claim follows from the linearity of D.

iii) If we have m such that $f(m) \equiv 0 \pmod{p^k}$, then there exists $\ell \in \mathbb{Z}$ such that $f(m) = \ell p^k$. Thus

$$\begin{aligned}f(m+ap^k) &\equiv f(m) + ap^k (Df)(m) \pmod{p^{k+1}} \\ &\equiv \ell p^k + ap^k (Df)(m) \pmod{p^{k+1}}\end{aligned}$$

$$\equiv (\ell + a(Df)(m))\, p^k \pmod{p^{k+1}}$$

which will be equivalent to 0 if

$$\ell + a(Df)(m) \equiv 0 \pmod{p}.$$

As $(Df)(m) \not\equiv 0 \pmod{p}$, we can solve this for $a \pmod{p}$, and take a to be the representative of this equivalence class in $0 \leq a < p$.

iv) By the previous part of the question, if such an $m = m_1$ exists, then there exists an m_2 such that

$$f(m_2) \equiv 0 \pmod{p^2}$$

and furthermore that $m_2 \equiv m_1 \pmod{p}$, and so

$$(Df)(m_2) \not\equiv 0 \pmod{p}.$$

Applying the results of the previous part again, we construct $m_3 \equiv m_2 \pmod{p}$ satisfying the conditions required, and so on, constructing $m_{k+1} \equiv m_k \pmod{p}$ for every $k \in \mathbb{N}$ as needed.

v) This is not sufficient for f to have an integer solution, as we have no guarantee that $\{m_k\}$ converges. Indeed, m_k will usually grow infinitely (unless we introduce p-adic numbers, but that is a discussion for another day), and so we cannot construct an integer solution in this way. For example $f(x) = x^2 + 1$, satisfies $f(3) \equiv 0 \pmod{5}$, and $(Df)(3) \equiv 2 \pmod{5}$, but $x^2 = 1$ has no real roots, let alone integer ones.