Tutorial 7

1. Given that 137 is a prime, use Gauss’s method to find \( x \in \mathbb{Z}_{137} \) such that \( x^2 \equiv -1 \) (mod 137).

Solution.

There is a square root of -1 modulo 137 which is smaller than \( \frac{137-1}{2} = 68 \). Hence there is an number \( x \leq 68 \), such that \( x^2 + 1 = 137k \), and so \( k \leq 33 \). Possible values of \( k \):

\[
1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \\
13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \quad 21 \quad 22 \quad 23 \quad 24 \\
25 \quad 26 \quad 27 \quad 28 \quad 29 \quad 30 \quad 31 \quad 32 \quad 33.
\]

Now reading \( x^2 + 1 = 137k \) modulo 3 we have \( x^2 + 1 \equiv 2k \) (mod 3) and so \( k \equiv 1 \) or 2 (mod 3).

This eliminates all multiples of 3 as a possible value of \( k \).

Now read \( x^2 + 1 = 137k \) modulo 4. We get \( x^2 + 1 \equiv k \) (mod 4) and so \( k \equiv 1 \) or 2 (mod 4).

This eliminates all values of \( k \equiv 0 \) or 3 (mod 4).

Similarly \( k \not\equiv 0, 1 \) or 2 (mod 5).

This leaves the following possibilities for \( k \), namely:

\( k = 1, 2, 5, 10, 17, 22, 25, 26 \)

It follows that \( k = 10 \) and \( x = \pm 37 \) (mod 137).

2. Given that 167 is a prime and that 3 is a square modulo 167, use a similar method to that in the preceding exercise to solve \( x^2 \equiv 3 \) (mod 167).

Solution.

If \( x^2 - 3 \equiv 0 \) (mod 167), then \( x^2 - 3 = 167k \) and we can assume that \( x \leq 83 \) and so that \( k \leq 41 \). Possible values for \( k \):

\[
1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \\
11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \\
21 \quad 22 \quad 23 \quad 24 \quad 25 \quad 26 \quad 27 \quad 28 \quad 29 \quad 30 \\
31 \quad 32 \quad 33 \quad 34 \quad 35 \quad 36 \quad 37 \quad 38 \quad 39 \quad 40 \quad 41.
\]

Now read \( x^2 - 2 = 167k \) modulo 3. We get \( x^2 - 3 \equiv x^2 \equiv -k \) (mod 3) and so \( k \equiv 2 \) or 0 (mod 3).

Hence we can eliminate all values of \( k \equiv 1 \) (mod 3).

Now read \( x^2 - 3 = 167k \) modulo 4.

We get \( x^2 - 3 \equiv -k \) (mod 4) and so \( k \equiv 2 \) or 3 (mod 4). Hence we can eliminate all values of \( k \equiv 0 \) or 1 (mod 4).
Similarly \( x^2 - 3 \equiv 2k \pmod{5} \) gives \( k \neq 0 \) or \( 2 \pmod{5} \).

We are left with the following possible values for \( k \):

\[ 3, 6, 11, 14, 18, 23, 26, 38, 39. \]

\( k = 23 \) works and gives \( \sqrt{3} = \pm 62 \in \mathbb{Z}_{167} \).

3.  

(i) Find the length of the periodic and non-periodic parts of the decimal expansion of

\[
\frac{45}{89}, \quad \frac{39}{24.5^2.103}.
\]

(ii) Use your calculators to find the decimal expansions of the above two numbers.

Solution.

For \( \frac{45}{89} \), the decimal expansion has no non-periodic part and a periodic part of length \( m = \text{ord}_{89}(10) = 44 \).

Its decimal expansion is 0.50561797752808988764044943820224719101123595.

For \( \frac{39}{24.5^2.103} \) the non-periodic part has length \( l = \max(4, 2) = 4 \), while the periodic part has length \( m = \text{ord}_{103}(10) \).

Now the order of 10 modulo 103 is a divisor of \( \varphi(103) = 102 \) and so is one of 1, 2, 3, 6, 17, 34, 51 or 102. In this case it is \( m = 34 \).

The decimal representation of \( \frac{39}{24.5^2.103} = 0.009466019417457281553398058252427184 \).

4.  Write the following numbers as rationals \( \frac{p}{q} \):

\[ 0 \cdot 5138273, \quad 0 \cdot 5130273. \]

Solution.

\[
0.5138273 = \frac{5138}{10^4} + \frac{273}{10^7} + \frac{273}{10^{10}} + \ldots \}
= \frac{5138}{10^4} + \frac{273}{10^7}(1 + \frac{1}{10^3} + \frac{1}{10^6} + \ldots )
= \frac{5138}{10^4} + \frac{273}{10^7} \frac{10^3}{10^3 - 1}
= \frac{1}{10^4} \{5138 + \frac{273}{999}\}
= \frac{1}{10^4} \frac{1710954}{333}
\]
Suppose that $\frac{p}{q}$, where $(p, q) = 1$, has a decimal representation whose periodic part has length 4. What can you say about the denominator $q$?

Solution.

Suppose that
\[ x = \frac{p}{q} = a_0 a_1 \ldots a_k.b_1 b_2 \ldots b_l c_1 c_2 c_3 c_4. \]

Now as in the above example,
\[
\begin{align*}
x &= \frac{a_0 a_1 \ldots a_k b_1 b_2 \ldots b_l}{10^l} + \\
&\quad \frac{c_1 c_2 c_3 c_4}{10^{l+4}} \{1 + \frac{1}{10^4} + \frac{1}{10^8} + \ldots\} \\
&= \frac{a_1 a_2 \ldots a_k b_1 b_2 \ldots b_l}{10^l} + \frac{(c_1 c_2 c_3 c_4) 10^4}{10^{l+4}(10^4 - 1)}.
\end{align*}
\]

Note that the denominator of this rational number is a divisor of $10^l(10^4 - 1)$.

For example,
\[
\frac{1}{101} = 0.009900990099 \ldots,
\]
\[
\frac{1453}{119901} = .145314531453 \ldots.
\]

6. Prove that
\[ x = 0.123456789101112131415161718192021 \ldots \]

is not rational.

Solution.

Suppose that $x = \frac{p}{q}$ is rational. Then its decimal expansion contains a periodic part of length $m$, since the decimal expansion of $x$ certainly doesn’t terminate.

Thus after a finite non-periodic distance $l$, there is a repeating block of length $m$. Now consider the number $n = 10^{l+2m+1} + 1$. The decimal representation of $x$ has a 1 followed by $l + 2m$ zeros followed by a 1. It follows that in the decimal expansion of $x$ the periodic block of length which occurs after an initial $l$ places must occur appear within the $l + 2m$ zeros. Thus the repeating block must consist entirely of zeros and so the decimal expansion of $x$ must end in a string of zeros. This is obviously not the case.
7. (Harder exercise)

(i) Let \( \omega \) be a complex cube root of 1, not 1. Show that \( \omega = \frac{-1 \pm \sqrt{-3}}{2} \) and that
\[ 1 + \omega + \omega^2 = 0. \]
You may assume that arithmetic in \( \mathbb{Z}[\omega] \) is exactly similar to arithmetic in \( \mathbb{Z}[i] \) or \( \mathbb{Z} \). Define
\[ N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2. \]

(ii) Calculate \( N(13 + 15\omega) \).

(iii) Show that there are exactly 6 units in \( \mathbb{Z}[\omega] \), namely \( \pm 1, \pm \omega, \pm \omega^2 = \pm (-1 - \omega) \).

(iv) Prove that 3 is not prime in \( \mathbb{Z}[\omega] \) by exhibiting a factorisation of it \( a la 2 \in \mathbb{Z}[i] \).

(v) Show that 2 is prime in \( \mathbb{Z}[\omega] \).

Solution.

(i) (i) Clear.

(ii) \[ N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2. \]
and that
\[ \bar{\omega} = \omega^2. \]
\[ N(13 + 15\omega) = 13^2 - 13.15 + 15^2 = 199. \]
Notice that this is a prime in \( \mathbb{Z} \). It should follow that \( 13 + 15\omega \) is prime in \( \mathbb{Z}[\omega] \).

(iii) Each of \( \pm 1, \pm \omega, \pm \omega^2 \) is a unit.
Conversely, let \( x = a + b\omega \) be a unit in \( \mathbb{Z}[\omega] \). Then there exists an element \( y \in \mathbb{Z}[\omega] \) such that \( xy = 1 \).
Then \( N(xy) = N(x)N(y) = 1 \) and since \( N(x), N(y) \) are both positive integers, it follows that \( N(x) = N(y) = 1 \).
Thus
\[ N(x) = a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 = 1. \]
Hence
\[ (2a - b)^2 + 3b^2 = 4 \]
as \( a, b \) are both integers.
It follows that either \( 2a - b = \pm 1 \), and \( b = \pm 1 \) or \( b = 0 \) and \( 2a - b = 2a = \pm 2 \).
The second case leads to the units \( x = \pm 1 \), while the first case leads to the possibilities:
\( b = 1, a = 0 \) and \( x = \omega \) or \( b = 1, a = 1 \) and \( x = 1 + \omega = -\omega^2; \)
\( b = -1, a = 0 \) and \( x = -\omega \) or \( b = -1, a = -1 \) and \( x = -1 - \omega = \omega^2. \)
We have thus listed all units in \( \mathbb{Z}[\omega] \). There are 6 of them: \( \pm 1, \pm \omega, \pm \omega^2. \)
Hence
\[ \mathbb{Z}[\omega]^* = \{ \pm 1, \pm \omega, \pm \omega^2 \}. \]

(iv) Note that
\[ 3 = -\sqrt{-3}\sqrt{-3} = -(2\omega + 1)^2. \]
Remember that $\omega = \frac{-1 + \sqrt{-3}}{2}$ and so $\sqrt{-3} = \pm(2\omega + 1)$.

Since $1 + 2\omega \notin \mathbb{Z}[\omega]^*$, it follows that 3 is not prime in $\mathbb{Z}[\omega]$.

(iii) Suppose that
\[ 2 = (a + b\omega)(c + d\omega) \in \mathbb{Z}[\omega]. \]

Then, taking complex conjugates, we have
\[ 2 = (a + b\omega^2)(c + d\omega^2). \]

Now we can multiply the above two equations together to get that
\[ 4 = (a^2 - ab + b^2)(c^2 - cd + d^2). \]

This is an equation in $\mathbb{Z}$.

There are then only three possibilities:

Either $a^2 - ab + b^2 = 1$ and $c^2 - cd + d^2 = 4$, or
$a^2 - ab + b^2 = 4$ and $c^2 - cd + d^2 = 1$, or
$a^2 - ab + b^2 = c^2 - cd + d^2 = 2$.

If $a^2 - ab + b^2 = 1$, then arguing exactly as in part (ii) it follows that $a + b\omega \in \mathbb{Z}[\omega]^*$ and is a unit. This implies that the factorisation $2 = (a + b\omega)(c + d\omega)$ involves the term $a + b\omega$ as a unit.

Similarly, if $c^2 - cd + d^2 = 1$, then $c + d\omega$ is a unit.

The only possibility which might be of interest is that
\[ a^2 - ab + b^2 = c^2 - cd + d^2 = 2. \]

But then we have
\[ (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 = 2 \]
and then
\[ (2a - b)^2 + 3b^2 = 8. \]

This is an equation in integers. It is easy to see that there are no integers which solve this equation.

It follows that any factorisation of 2 in $\mathbb{Z}[\omega]$ involves a unit and so 2 is a prime in $\mathbb{Z}[\omega]$. 