1. Use your hand calculator to find the exact decimal expansion of $\frac{49}{97}$.

Solution

My calculator gives:

$$\frac{49}{97} = 0.5051546392.$$  

I can presumably be reasonably sure that all the digits are correct, except possibly the last digit, because I don’t know whether this pesky calculator has rounded the representation off. So the number might have been one of the following:

- 0.50515463924
- 0.50515463917
- 0.5051546392003

This last might have occurred if my calculator showed exactly 12 digits and has presented 0.505154639200 as 0.5051546392, because it presumes that I’m not interested in the last 00, for some peculiar reason.

In any event, I can’t be very sure about the last digit at all. So I remove the last two digits to be on the safe side, and consider the number 0.505154639. This number is definitely less than $\frac{49}{97}$ and so if I multiply it by 97 I will definitely get a number smaller than 49. In fact I get 48.99999911.

If you think that the calculator is dividing 97 into 49 by the olde school algorithm, this number is trying to tell you what the remainder was when it calculated the third last digit 3. That remainder is 89, which is what we need to add to 48.99999911 to get exactly 49. Now divide 89 by 97 with the calculator. I get .9175257732. We see that my calculator in fact rounded off the last digit to present me with a 2, in the first calculation. Then the fraction $\frac{49}{97}$ is actually

$$0.5051546391752577,$$

where again we can’t be sure of the last 2.

Repeat the process. We get:

$$0.91752577 \times 97 = 88.99999969$$

and so the remainder is 31 and we need

$$\frac{31}{97} = 0.3195876289,$$

and

$$\frac{49}{97} = 0.50515463917525773195876289,$$
where again we can’t be sure of the last digit. The correct expansion for $\frac{49}{97}$ is:

$$
0.
\begin{array}{cccccccc}
5051 & 5463 & 9175 & 2577 \\
3195 & 8762 & 8865 & 9793 \\
8144 & 3298 & 9690 & 7216 \\
4948 & 4536 & 0824 & 7422 \\
6804 & 1237 & 1134 & 0206 \\
1855 & 6701 & 0309 & 2783 \\
\vdots
\end{array}
$$

where the expansion repeats with the same pattern with a period of 96. Notice the fact that the first and fourth rows are complementary in that corresponding digits sum to 9. This continues for the second and fifth rows and the third and sixth rows. You could try to think about why that is.

2. (a) Without actually evaluating the decimal expansions involved, find the length of the periodic and non-periodic parts of the decimal expansion of $\frac{45}{89}$, $\frac{39}{2^{4}.5^{2}.103}$.

(b) Use your calculator to find the decimal expansions of $\frac{45}{89}$.

**Solution**

For $\frac{45}{89}$, the decimal expansion has no non-periodic part and a periodic part of length $m = \text{ord}_{89}(10) = 44$. One finds this by calculating the following powers of 10 modulo 89:

$$
n \quad 1 \quad 2 \quad 4 \quad 8 \quad 11 \quad 22 \quad 44 \quad 88 \\
10^n \quad 10 \quad 11 \quad 32 \quad 45 \quad 55 \quad 88 \quad 1.
$$

Its decimal expansion is $0.5056179775280898876404943820224719101123595$.

For $\frac{39}{2^{4}.5^{2}.103}$, 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 $m = 34$. One finds this by calculating the following powers of 10 modulo 103:

$$
n \quad 1 \quad 2 \quad 3 \quad 6 \quad 17 \quad 34 \quad 51 \quad 102 \\
10^n \quad 10 \quad -3 \quad -30 \quad 76 \quad 102 \quad 1.
$$

The decimal representation is actually:

$$
\frac{39}{2^{4}.5^{2}.103} = 0.0009466019417457281553398058252427184.
$$

3. Write the following numbers as rationals $\frac{p}{q}$:

$$
0.513\overline{873} \quad 0.513\overline{073}.
$$

**Solution**
4. Suppose that \( \frac{p}{q} \), where \((p, q) = (q, 10) = 1\) has a decimal representation whose periodic part has length 4. What is the order of 10 modulo \( q \)? What can you say about the denominator \( q \)?

**Solution**

Suppose that

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

By Theorem 15.1, in the decimal expansion of \( x = \frac{p}{q} \), the periodic part has length \( \text{ord}_q(10) \) and so \( \text{ord}_q(10) = 4 \). Hence \( 10^4 - 1 \equiv 0 \pmod{q} \) and so \( q \) divides 9999 = 9.11.101. Hence \( q \in \{1, 3, 9, 11, 33, 99, 101, 3.101, 9.101, 11.101, 33.101, 99.101\} \). If \( q \) divides 10 - 1, \( \text{ord}_q(10) = 1 \) and the decimal expansion has a repeating block of length 1. If \( q \) divides \( 10^2 - 1 \), then \( \text{ord}_q(10) \leq 2 \) and the decimal expansion has a repeating block of length \( \leq 2 \). Hence the only possible values of \( q \) are

\[
\]
Rational numbers with these denominators have repeating block of length 4. For example,
\[
\begin{align*}
\frac{25}{101} &= 0.2475 \\
\frac{250}{303} &= 0.8250 \\
\frac{250}{909} &= 0.2750 \\
\frac{257}{1111} &= 0.2313 \\
\frac{2572}{3333} &= 0.7716 \\
\frac{2572}{9999} &= 0.2572
\end{align*}
\]

5. Given that 2 is a primitive root modulo 101, write down all elements \(x \in \mathbb{Z}_{101}\) which satisfy \(x^{10} = 1 \in \mathbb{Z}_{101}\).

**Solution**

\(\text{ord}_{101}(2) = 100\) and so the elements of \(\mathbb{Z}_{101}\) which have order 10 are
\[
\begin{align*}
2^{10} &= 14 \\
2^{20} &= 95 \\
2^{30} &= 17 \\
2^{40} &= 36 \\
2^{50} &= -1 = 100 \\
2^{60} &= -14 = 87 \\
2^{70} &= -95 = 6 \\
2^{80} &= -17 = 84 \\
2^{90} &= -36 = 65 \\
2^{100} &= 1 \in \mathbb{Z}_{101}.
\end{align*}
\]

6. Prove that 
\[x = 0.12345678910112131415161718192021\ldots\]
is not rational.

**Solution**

Suppose that \(x = p/q\) 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 \(n\) 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. Use Fermat’s Method of descent to write the prime 2473 as a sum of two squares. (You are given that $567 = \sqrt{-1} \in \mathbb{Z}_{2473}$.)

**Solution**

First $567^2 + 1 = 2473.130$. Reading this modulo 130 we have $47^2 + 1^2 = 130.17$. Hence we have

$$567^2 + 1^2 = 2473.130$$
$$47^2 + 1^1 = 17.130,$$
and so

$$(567^2 + 1^2)(47^2 + (-1)^2) = (567.47 - 1(-1) + 1.47)^2$$
$$= 26650^2 + 520^2 = 130^2.17.2473.$$

Dividing by $130^2$ we have

$$205^2 + 4^2 = 2473.17.$$

Now repeat the process. We get

$$205^2 + 4^2 = 2473.17$$
$$1^2 + (-4)^2 = 17,$$
and so

$$(205^2 + 4^2)(1^2 + (-4)^2) = 2473.17^2$$
$$(205.1 - 4(-4))^2 + 205(-4) + 4.1)^2 = 2473.17^2$$
$$221^2 + 816^2 = 2473.17^2.$$

Dividing by $17^2$ we have

$$13^2 + 48^2 = 2473.$$

8. (Harder question) 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

$$N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2.$$

(a) Calculate $N(13 + 15\omega)$.

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

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

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

(e) Show that if $p \in \mathbb{Z}$ is a prime $\equiv 2 \pmod{3}$, then $p$ remains prime in $\mathbb{Z}[\omega]$.

**Solution**

(a)

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

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 $\mathbb{Z}[\omega]$. 
(b) 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
$$(2a-b)^2 + 3b^2 = 4$$and $a, b$ 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
$$\mathbb{Z}[\omega]^* = \{\pm 1, \pm \omega, \pm \omega^2\}.$$It is now clear that $13 + 15\omega$ is a prime in $\mathbb{Z}[\omega]$, because if we could write
$$13 + 15\omega = (a + b\omega)(c + d\omega),$$then
$$N(13 + 15\omega) = 199$$
$$= N(a + b\omega)N(c + d\omega).$$This last equation is an equation in $\mathbb{Z}$ and since 199 is a prime in $\mathbb{Z}$, it follows that either $N(a + b\omega) = 1$ or $N(c + \omega) = 1$. These possibilities ensure that either $a + b\omega$ is a unit or $c + d\omega$ is a unit and so any factorisation of $13 + 15\omega$ in $\mathbb{Z}[\omega]$ must involve a unit.

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

(d) 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 \(\mathbb{Z}[\omega]\).

(e) If \(p = (a + b\omega)(c + d\omega)\), then
\[p^2 = N(p) = N(a + b\omega)N(c + d\omega) = (a^2 - ab + b^2)(c^2 - cd + d^2)\]
This is an equation in \(\mathbb{Z}\) and so we must have
\[a^2 - ab + b^2 = 1 \text{ and } c^2 - cd + d^2 = p^2, \text{ or}\]
\[a^2 - ab + b^2 = p^2 \text{ and } c^2 - cd + d^2 = 1, \text{ or}\]
\[a^2 - ab + b^2 = c^2 - cd + d^2 = p.\]
In the first case, it follows that \(a + b\omega\) is a unit if \(\mathbb{Z}[\omega]\); in the second case, we have \(c + d\omega\) is a unit in \(\mathbb{Z}[\omega]\); the last case cannot arise, because the squares modulo 3 are 0 and 1 and so
\[a^2 - ab + b^2 \equiv 0 - 0 + 0 \equiv 0 \pmod{3} \text{ or}\]
\[
\equiv 1 - 1 + 1 \equiv 1 \pmod{3} \\
\not\equiv 2 \pmod{3}.
\]
Hence we have found many primes (in fact infinitely many) in \(\mathbb{Z}[\omega]\), namely
\[2, 5, 11, 17, 23, 29, 41, \ldots.\]
If \(a^2 - ab + b^2 = p \equiv 2 \pmod{3}\), then