**Week 9**

## 12.2 The value of $(2/p)$

**Theorem 12.2** *If $p$ is an odd prime, then*

$$(2/p) = \begin{cases} 1 & \text{iff } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{iff } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

**Proof.** We apply Gauss's Lemma. We must find out how many of the least residues (mod $p$) of

$$2, 4, 6, ..., 2\left(\tfrac{p-1}{2}\right) \tag{12.4}$$

are greater than $\frac{p-1}{2}$. But all $\frac{p-1}{2}$ of these numbers lie between 2 and $p-1$, so they are all least residues, and we only have to find out how many of them are greater than $\frac{p-1}{2}$. Note that they are all even. Which is the first even number greater than $\frac{p-1}{2}$? To find out, we need to know whether $\frac{p-1}{2}$ is even or odd.

★ Suppose $\frac{p-1}{2}$ is even. Then $\frac{p-1}{2} = 2m$ for some $m$, so that $p-1 = 4m$, and the first even number greater than $2m$ is $2m+2$. Thus all numbers in (12.4) greater than $2m$ are

$$2m+2, 2m+4, ..., 4m. \tag{12.5}$$

There are

$$\frac{4m-(2m+2)}{2} + 1 = m$$

numbers in (12.5).

⋆ If $m$ is even, thus if $m = 2n$ for some $n$, then by Gauss's Lemma,

$$(2/p) = (-1)^{2n} = 1.$$

In this case

$$p = 4m+1 = 8n+1$$

and so $p \equiv 1 \pmod 8$.

⋆ If $m$ is odd, thus if $m = 2n+1$ for some $n$, then

$$(2/p) = (-1)^{2n+1} = -1.$$

In this case

$$p = 4m+1 = 8n+5$$

and so $p \equiv 5 \pmod 8$.

★ Suppose $\frac{p-1}{2}$ is odd. Then $\frac{p-1}{2} = 2m+1$ for some $m$, so that $p-1 = 4m+2$, and the first even number greater than $2m+1$ is also $2m+2$. Thus all numbers in (12.4) greater than $2m+1$ are

$$2m+2, 2m+4, ..., 4m, 4m+2. \tag{12.6}$$

There are

$$\frac{4m+2-(2m+2)}{2} + 1 = m+1$$

numbers in (12.6).

⋆ If $m+1$ is even, thus if $m+1 = 2n$ for some $n$, then

$$(2/p) = (-1)^{2n} = 1.$$

Now $m = 2n-1$, hence

$$p = 4m+3 = 4(2n-1)+3 = 8n-1$$

and so $p \equiv -1 \equiv 7 \pmod 8$.

- ⋆ If $m+1$ is odd, thus if $m$ is even, say $m = 2n$ for some $n$, then

$$(2/p) = (-1)^{m+1} = (-1)^{2n+1} = -1.$$

We have

$$p = 4m+3 = 8n+3$$

and so $p \equiv 3 \pmod 8$. ■

We also prove the following application of Theorem 12.2.

**Theorem 12.3** *If $p$ and $q = 4p+1$ are both primes, then 2 is a primitive root of $q$.*

**Proof.** Because $q$ is prime, $\phi(q) = q-1 = 4p$.

- By Theorem 10.2, $\operatorname{ord}_q 2$ is a divisor of $4p$, so the order of 2 is one of 1, 2, 4, $p$, $2p$, or $4p$.
- We show that the first five cases are impossible.

- ▼ First consider $2p$. What is $2^{2p}$? Note that $q = 4p + 1$, so $2p = \frac{q-1}{2}$.
  By Euler's Criterion, we have

$$2^{2p} \equiv 2^{(q-1)/2} \equiv (2/q) \pmod{q}.$$

  ▼ What is $(2/q)$? To find out, we must determine the least residue of $q \pmod 8$.
  We know $p$ is odd; say $p = 2k + 1$ for some $k$. Then $4p = 8k + 4$, that is, $4p \equiv 4 \pmod 8$ and so $q \equiv 4 + 1 \equiv 5 \pmod 8$. By Theorem 12.2, $(2/q) = -1$ and so

$$2^{2p} \equiv (2/q) \equiv -1 \pmod{q}.$$

  Therefore $\text{ord}_q 2 \neq 2p$.

  ▼ Let $d$ be any divisor of $2p$. Then 2 cannot have order $d$, for if it had, Theorem 10.1 would imply that $2^{2p} \equiv 1 \pmod q$ which is not the case.
  Therefore $\text{ord}_q 2 \notin \{1, 2, p\}$.

  ▼ Suppose $\text{ord}_q 2 = 4$. Then

$$1 \equiv 2^4 \equiv 16 \pmod{q}$$

  and so $q|15$. Since $q$ is a prime of the form $4p + 1$, the only possibility is $q = 5$. But then $p = 1$, which is not the case as $p$ is prime. Hence $\text{ord}_q 2 \neq 4$.

Therefore $\text{ord}_q 2 = 4p$ and by definition 2 is a primitive root of $q$. ■

## 12.3 Equivalent Form of the Quadratic Reciprocity Theorem

Here is another form (equivalent to the previous one) of the Quadratic Reciprocity Theorem:

If $p$ and $q$ are odd primes, then

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

Hence the QRT links $(p/q)$ and $(q/p)$ via their **product**. Gauss's Lemma gives us a way of calculating

1. $(q/p)$ by using a property of the numbers $q, 2q, ..., \frac{p-1}{2}q$, and
2. $(p/q)$ by using a property of the numbers $p, 2p, ..., \frac{q-1}{2}p$.

# Section 13

# Numbers in other bases

We write integers in place-value notation, with each place indicating a different power of 10. The first people to use place-value notation were the Babylonians of more than 3000 years ago. The Babylonians transmitted the idea to the Hindus before 600 BC, who passed it on (by 600 AD) to the Arabs, from where it spread to Europe (by 1200 AD).

There is no reason why 10 must be used for place-value notation; any other integer bigger than 1 will also work. Several other integers have in fact be used for this purpose – we call such an integer a **base** of the place-value notation.

In this section we look at integers in bases other than 10.

## 13.1 Writing Base 10 Integers in Other Bases

The first two theorems in this section are direct consequences of the third theorem and are stated without proof.

**Theorem 13.1** *Every positive integer can be written as a sum of distinct powers of* 2.

**Theorem 13.2** *Every positive integer can be written as a sum of distinct powers of* 2 *in only one way.*

**Theorem 13.3** *Let $b \geq 2$ be any integer, called the base. Every positive integer $n$ can be written uniquely in the base $b$, that is, in the form*

$$n = d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k$$

*for some $k$, with $0 \leq d_i < b$, $i = 0, 1, ..., k$.*

**Proof.**
Divide $n$ by $b$. By the division algorithm, there exist unique integers $q_1$ and $d_0$ such that

$$n = q_1 b + d_0, \quad 0 \le d_0 < b.$$

Divide the quotient $q_1$ by $b$; by the division algorithm, there exist unique integers $q_2$ and $d_1$ such that

$$q_1 = q_2 b + d_1, \quad 0 \le d_1 < b,$$

and continue the process,

$$q_2 = q_3 b + d_2, \quad 0 \le d_2 < b,$$
$$\vdots$$

and so on. Since $n > q_1 > q_2 > q_3 \cdots$ and each $q_i$ is nonnegative, the sequence $n > q_1 > q_2 > q_3 \cdots$ eventually terminates (Well-Ordering Principle). That is, there is an integer $k$ such that

$$q_k = 0 \cdot b + d_k, \quad 0 \le d_k < b.$$

Then

$$\begin{array}{rcl} n &=& d_0 + q_1 b = d_0 + (q_2 b + d_1) b \\ &=& d_0 + d_1 b + (q_3 b + d_2) b^2 \\ &\vdots& \\ &=& d_0 + d_1 b + d_2 b^2 + \cdots + d_{k-1} b^{k-1} + q_k b^k \\ &=& d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k, \end{array} \qquad \begin{array}{rcl} &=& d_0 + d_1 b + q_2 b^2 \\ &=& d_0 + d_1 b + d_2 b^2 + q_3 b^3 \\ &\vdots& \end{array}$$

and this is the desired representation. The uniqueness of this representation follows from the fact that, by the division algorithm, each $q_i$ and $d_i$ are unique. ■

We write $d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k$ as $(d_k d_{k-1} \ldots d_1 d_0)_b$.

**Example:** Write 1492 in base 3.

**Solution**

| Quotients | Remainders |
|---|---|
| $3 \overline{)1492}$ | |
| 497 | 1 |
| 165 | 2 |
| 55 | 0 |
| 18 | 1 |
| 6 | 0 |
| 2 | 0 |
| 0 | 2 |

Hence $1492 = 2001021_3$.

## 13.2 Converting Integers in Other Bases to Base 10

**Example:** Write $3141_5$ in base 10.

**Solution:** $3141_5 = 3 \cdot 5^3 + 1 \cdot 5^2 + 4 \cdot 5 + 1 = 3 \cdot 125 + 25 + 21 = 421$.

## 13.3 Working in Other Bases

**Example:** The numbers below are given in base 9. Calculate, in base 9 (that is, no conversion to base 10 or any other base)

$$35 + 24 + 33.$$

**Solution**

In base 9 there are only nine digits: $0, 1, 2, ..., 8$, and $8 + 1 = 10$. So if we count in base 9, we would count $1, 2, ..., 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, ...$, etc. Thus

$$\begin{aligned} 35 + 24 + 33 &= ((5 + 4) + 3) + (30 + 20 + 30) \\ &= (10 + 3) + (30 + 20 + 30) \\ &= (10 + 30 + 20 + 30) + 3 \\ &= 100 + 3 = 103. \end{aligned}$$

## 13.4 Decimals in Other Bases

**Example:** Let $(.d_1d_2d_3...)_b$ stand for $d_1/b + d_2/b^2 + d_3/b^3 + \cdots$. Evaluate $(.444...)_9$ as rational number in base 10.

**Solution**

$$(.444...)_9 = 4/9 + 4/9^2 + 4/9^3 + \cdots .$$

But we know that if $r$ is a positive integer and $a > 1$, then

$$1 + a^{-r} + a^{-2r} + \cdots = \frac{1}{1 - a^{-r}}.$$

Hence

$$\begin{aligned} 4/9 + 4/9^2 + 4/9^3 + \cdots &= \frac{4}{9}(1 + 1/9 + 1/9^2 + 1/9^3 + \cdots) \\ &= \frac{4}{9} \cdot \frac{1}{1 - \frac{1}{9}} \\ &= \frac{4}{9} \cdot \frac{9}{8} = \frac{1}{2}. \end{aligned}$$

# Section 14

# Duodecimals

This is about arithmetic in base 12. Read it for interest sake; I will not discuss it in class.

# Section 15

# Decimals

Some fractions, like $\frac{1}{2} = 0.5$, have simple decimal expansions, others, like $\frac{1}{3} = 0.333...$ have slightly more complicated expansions, while others, like $\frac{1}{17} = 0.0588235294117647...$ have very complicated decimal expansions. In this section we will see which fractions have the simplest expansions (and why), and find out how long the **period** – the repeating part of a repeating decimal – is without actually finding the expansion.

- Note that any rational number has a decimal expansion that either terminates or repeats.

## 15.1 Terminating Decimal Expansions

Look at the table of the decimal expansions of $1/n$, for $n = 2, ..., 29$:

| $n$ | $1/n$ | Period | | $n$ | $1/n$ | Period |
|---|---|---|---|---|---|---|
| 2 | .5 | 0 | | 16 | .0625 | 0 |
| 3 | $.\overline{3}$ | 1 | | 17 | $.\overline{0588235294117647}$ | 16 |
| 4 | .25 | 0 | | 18 | $.0\overline{5}$ | 1 |
| 5 | .2 | 0 | | 19 | $.\overline{052631578947368421}$ | 18 |
| 6 | $.1\overline{6}$ | 1 | | 20 | .05 | 0 |
| 7 | $.\overline{142857}$ | 6 | | 21 | $.\overline{047619}$ | 6 |
| 8 | .125 | 0 | | 22 | $.0\overline{45}$ | 2 |
| 9 | $.\overline{1}$ | 1 | | 23 | $.\overline{0434782608695652173913}$ | 22 |
| 10 | .1 | 0 | | 24 | $.041\overline{6}$ | 1 |
| 11 | $.\overline{09}$ | 2 | | 25 | .04 | 0 |
| 12 | $.08\overline{3}$ | 1 | | 26 | $.0\overline{384615}$ | 6 |
| 13 | $.\overline{076923}$ | 6 | | 27 | $.\overline{037}$ | 3 |
| 14 | $.0\overline{714285}$ | 6 | | 28 | $.03\overline{571428}$ | 6 |
| 15 | $.06\overline{}$ | 1 | | 29 | $.\overline{0344827586206896551724137931}$ | 28 |

Table 15.1: Decimal expansion of $1/n$, for $n = 2, ..., 29$

The integers in the table whose reciprocals have terminating decimal expansions are 2, 4, 5, 8, 10, 16, 20, and 25. What do these numbers have in common? They are all of the form $2^a5^b$ for some nonnegative integers $a$ and $b$. This is true in general, and these are also the *only* integers whose reciprocals have terminating decimal expansions.

We now prove that the positive integers with terminating decimal expansions are precisely the numbers of the form $2^a5^b$ for some nonnegative integers $a$ and $b$.

**Theorem 15.1** *If $a$ and $b$ are nonnegative integers not both equal to 0, then the decimal expansion of $1/2^a5^b$ terminates. The expansion has $M$ digits, where $M = \max\{a, b\}$; that is, $1/2^a5^b = 0.d_1d_2...d_M$, where $d_M \neq 0$ (but possibly $d_1 = ... = d_i = 0$ for some $i < M$).*

**Proof.**
Let $M = \max\{a, b\}$. Then $M - a \geq 0$, $M - b \geq 0$, so

$$10^M(1/2^a5^b) = \frac{2^M5^M}{2^a5^b} = 2^{M-a}5^{M-b} \tag{15.1}$$

is an integer; call it $n$. Then $n < 10^M$, so we can write

$$\begin{aligned} n &= 10^{M-1}e_{M-1} + 10^{M-2}e_{M-2} + \cdots + 10^2e_2 + 10e_1 + e_0 \\ &= e_{M-1} \cdots e_2e_1e_0 \end{aligned}$$

in digital representation. Since $M = \max\{a, b\}$, at least one of $M - a$, $M - b$ is equal to 0. In particular, $n$ is not divisible by 10, so $e_0 \neq 0$. Now from (15.1),

$$\begin{aligned} \frac{1}{2^a5^b} &= \frac{n}{10^M} \\ &= \frac{e_{M-1} \cdots e_2e_1e_0}{10^M} \\ &= 0.e_{M-1} \cdots e_2e_1e_0, \end{aligned}$$

with $e_0 \neq 0$.
Let $d_i = e_{M-i}$, $i = 1, ..., M$. Then

$$\frac{1}{2^a5^b} = 0.d_1d_2 \cdots d_M,$$

$d_M \neq 0$. ■

**Theorem 15.2** *If $1/n$ has a terminating decimal expansion, then $n = 2^a5^b$ for some nonnegative integers $a$ and $b$.*

**Proof.**
Let the terminating decimal expansion of $1/n$ be

$$\begin{aligned} 1/n &= .d_1d_2...d_k \\ &= d_1/10 + d_2/10^2 + \cdots + d_k/10^k \\ &= \frac{\overbrace{d_1 10^{k-1} + d_2 10^{k-2} + \cdots + d_k}^{=\,m}}{10^k}. \end{aligned}$$

Let $m = d_1 10^{k-1} + d_2 10^{k-2} + \cdots + d_k$. Then $1/n = m/10^k$, that is, $mn = 10^k$. Hence $n|10^k$. But the only prime divisors of $10^k$ are 2 and 5, so the only prime divisors of $n$ are 2 and 5. Thus $n = 2^a 5^b$ for some nonnegative integers $a$ and $b$. ■

Note that if $1/n$ has a terminating decimal expansion, it also has a non-terminating expansion: Prove that $0.d_1d_2\cdots d_M = 0.d_1d_2\cdots(d_M - 1)999... = 0.d_1d_2\cdots(d_M - 1)\overline{9}$.

Theorems 15.1 and 15.2 can be generalized to expansions of reciprocals of integers in any base. The expansion of $1/n$ in base $b$ is $(.d_1d_2d_3...)_b$, where

$$1/n = d_1/b + d_2/b^2 + d_3/b^3 + ..., \ 0 \le d_k < b.$$

**Example:** Find the expansions of 1/2, 1/3 and 2/9 in base 6.

**Solution**
Note that $1/2 = 3/6$, $1/3 = 2/6$ and $2/9 = 8/36 = (6+2)/36 = 1/6 + 2/36$. Thus

$$\begin{aligned} 1/2 &= (.3)_6, \\ 1/3 &= (.2)_6, \\ 2/9 &= (.12)_6. \end{aligned}$$

**Theorem 15.2A** *The expansion of $1/n$ in the base $b$ terminates if and only if every prime divisor of $n$ is a divisor of $b$.*