# DISCRETE MATHEMATICS
## Math 245

Michael E. O'Sullivan

Suggestions for preparing for the Second Exam

(*) indicates level 2 problems.

I. Things you should know about the integers and rational numbers:

- Be able to use (and recognize that you are using) commutativity, associativity, the additive and multiplicative identity, the additive inverse (and, for the rationals, the multiplicative inverse), distributivity.
- Be able to use (and recognize that you are using ) properties of $<$. For example $a < b$ implies $a + c < b + c$.
- Be able to define prime, composite, divides, floor, ceiling.

II. The big theorems

- Know how to apply the following important theorems (as in webworks problems):
  - Quotient-remainder theorem.
  - The unique factorization theorem.
- * Know the precise statements of the theorems.

III. Be able to do these computations.

- Use the Euclidean algorithm to find the greatest common divisor of two numbers.
- Convert an integer (base 10) into another base, and convert from any base into base 10.
- Add in any given base.
- Construct a multiplication table in a given base.
- Use a multiplication table to find a product of two numbers in any given base.
- Use unique factorization to solve equations involving integers.
- Simplify expressions using the floor and ceiling functions.

IV. Know these standard proofs and proof methods.

- Divisibility results like:
  - Transitivity of divides.
  - If $a$ divides $b$ and $a$ divides $c$ then $a$ divides $b + c$.
  - When $a = bx + c$, $\gcd(a, b) = \gcd(b, c)$.

- *Proofs by contradiction:
  - There exist an infinite number of primes (by contradiction).
  - $\sqrt{p}$ is irrational for $p$ a prime (by contradiction).
  - The sum of a rational number and an irrational number is irrational.
- Floor and ceiling functions.
  - Be able to compute and simplify expressions.
  - Be able to give counterexamples to false statements.
  - Be able to write proofs using the definitions (as in Epp, 4th Ed. §4.5 , and 3rd Ed. Sec 3.5).
- In general, know how to use a counterexample to *disprove* a universal statement.

# Base $b$ representations and base $b$ arithmetic.

October 13, 2011

## 1 Converting between bases

Here is the main theorem.

**Theorem 1.1** (Base $b$). *Let $b$ be an integer with $b \geq 2$. For any $n \in \mathbb{N}$ there is a $t \geq 0$ and $a_0, a_1, a_2, \ldots, a_t$ with all $a_i \in \{0, 1, \ldots, b-1\}$ and $a_t \neq 0$ such that*

$$n = a_t b^t + a_{t-1} b^{t-1} + \cdots + a_1 b + a_0$$

*Furthermore, this expression for $n$ is unique.*

The integer $t$ indicates the number of terms in the base $b$ representation, $t + 1$. The integers $a_i$ are the base $b$, "digits" in the representation of $n$. The last sentence says that there is only one way to represent a number base $b$.

We can write a subscript on a number to indicate the base: so $345_8$ is the number $3*8^2+4*8+5$ whereas $345_{10}$ is the number $3 * 10^2 + 4 * 10 + 5$. We wouldn't write $345_5$ since the digit 5 is not allowed base 5. When the context is clear, we don't write the subscript. For example, usually we won't write base 10 numbers with a subscript, we will only use it when we need to be very clear that we are working base 10.

To convert from base $b$ to base 10 is easy, you just write down the powers of $b$ in base 10, and then use arithmetic base 10, which you learned in grade school.

$$\begin{aligned} 345_8 &= 3 * 8^2 + 4 * 8 + 5 \\ &= 3 * 64 + 4 * 8 + 5 \\ &= 192 + 32 + 5 \\ &= 229 \end{aligned}$$

The numbers without subscript are all base 10.

To convert from base 10 to base $b$ is a little trickier. The following algorithm is based on the quotient remainder theorem. We do a succession of divisions by $b$. Each remainder becomes one of the base $b$ digits. Each quotients is used in the following division step. Here is an example.

$$\begin{aligned}
47 &= 2 * 23 + 1 \qquad \text{so } a_0 = 1\\
23 &= 2 * 11 + 1 \qquad \text{so } a_1 = 1\\
11 &= 2 * 5 + 1 \qquad \text{so } a_2 = 1\\
5 &= 2 * 2 + 1 \qquad \text{so } a_3 = 1\\
2 &= 2 * 1 + 0 \qquad \text{so } a_4 = 0\\
1 &= 2 * 0 + 1 \qquad \text{so } a_5 = 1
\end{aligned}$$

We can stop because the last quotient was 0. Thus we have $45_{10} = 101111_2$. Let's check!

$$\begin{aligned}
101111_2 &= 1 * 32 + 0 * 16 + 1 * 8 + 1 * 4 + 1 * 2 + 1 * 1\\
&= 40 + 7 = 47
\end{aligned}$$

Yep!

Now let's convert to base 8.

$$\begin{aligned}
47 &= 8 * 5 + 7\\
5 &= 8 * 0 + 5
\end{aligned}$$

This shows $47_{10} = 57_8$. Check: $57_8 = 5 * 8 + 7 = 47_{10}$. Yep!

## 2 Bases that are powers of 2

Computers store data as sequences of 0's and 1's, so they store integers in base 2, also called binary. The digits are usually called bits. Since binary expressions are very long, we often write the a binary number using octal (base 8), or hexadecimal (base 16). In base 16, we use the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ (so $A_{16} = 10_{10}$, $B_{16} = 11_{10}, \ldots, F_{16} = 15_{10}$).

There is a simple way to convert from base 2 to base 4, 8, 16 (or any power of 2) without going through base 10. Let's consider base 8. Suppose that $n$ requires 9 digits base 2 digits bits). Write down the expression for $n$ base 2 and rearrange using the distributive law.

$$\begin{aligned}
n &= a_9 2^9 + a_8 2^8 + a_7 2^7 + a_6 2^6 + a^5 2^5 + a_4 2^4 + a_3 2^3 + a_2 2^2 + a_1 2 + a_0\\
&= a_9 2^9 + (a_8 2^2 + a_7 2 + a_6) 2^6 + (a^5 2^2 + a_4 2 + a_3) 2^3 + (a_2 2^2 + a_1 2 + a_0)\\
&= a_9 * 8^3 + (a_8 2^2 + a_7 2 + a_6) * 8^2 + (a^5 2^2 + a_4 2 + a_3) * 8 + (a_2 2^2 + a_1 2 + a_0)
\end{aligned}$$

Now each of the numbers $(a_8 2^2 + a_7 2 + a_6)$ and $(a_5 2^2 + a_4 2 + a_3)$ and $(a_2 2^2 + a_1 2 + a_0)$ is between 0 and 7. We get 0 when all the $a_i = 0$ and 7 when all the $a_i$ are 1. So this is our base 8 expansion.

An analogous method works for base 4; w group 2 digits together and convert the pair to base 4. For base 16, we group 4 digits together, and convert to base 16. Here are examples:

$$\begin{aligned}
11101111010_2 &= 11, 101, 111, 010_2 = 3572_8\\
11101111010_2 &= 1, 11, 01, 11, 10, 10_2 = 131322_4\\
11101111010_2 &= 111, 0111, 1010_2 = 77B_{16}
\end{aligned}$$

Similarly, we can convert from the bases 4, 8, and 16 to base 2 by expanding each digit, *using the appropriate number of bits for each.*

$$A7F9_{16} = 1010, 0111, 1111, 0101_2$$
$$56732_8 = 101, 110, 111, 011, 010_2$$

## 3 Base $b$ arithmetic

We will now look at arithmetic base $b$. This is essentially relearning what you learned in grade school! When we work base 8 it is as though you are allowed to count with your fingers, *not using your thumbs.* Students often find arithmetic base $b$ unsettling; it is very much like learning a new language.

Let's consider base 8 first. Let's start by counting. Since I've made clear that we are working base 8, I won't write the subscript 8 on each number. The first 8 numbers (starting with 0) are

$$0, 1, 2, 3, 4, 5, 6, 7$$

The next 8 numbers are

$$10, 11, 12, 13, 14, 15, 16, 17$$

The next numbers, in groups of 8 are

$$20, 21, 22, 23, 24, 25, 26, 27$$
$$30, 31, 32, 33, 34, 35, 36, 37$$
$$40, 41, 42, 43, 44, 45, 46, 47$$
$$50, 51, 52, 53, 54, 55, 56, 57$$
$$60, 61, 62, 63, 64, 65, 66, 67$$
$$70, 71, 72, 73, 74, 75, 76, 77$$
$$100, 101, 102, 103, 104, 105, 106, 107$$

The last number, in base 10 is $107_8 = 1 * 8^2 + 0 * 8 + 7 = 71$.

Now let's make an addition table and a multiplication table base 8.

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 10 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 10 | 11 |
| 3 | 3 | 4 | 5 | 6 | 7 | 10 | 11 | 12 |
| 4 | 4 | 5 | 6 | 7 | 10 | 11 | 12 | 13 |
| 5 | 5 | 6 | 7 | 10 | 11 | 12 | 13 | 14 |
| 6 | 6 | 7 | 10 | 11 | 12 | 13 | 14 | 15 |
| 7 | 7 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

To make a multiplication table, for row $r$ think about successive addtion by $r$, and use the list of numbers written base 8 that we have above. So for row 2, start with 0 and successively add 2. For row 3 start with 0 and succesively add 3.

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 10 | 12 | 14 | 16 |
| 3 | 0 | 3 | 6 | 11 | 14 | 17 | 22 | 25 |
| 4 | 0 | 4 | 10 | 14 | 20 | 24 | 30 | 34 |
| 5 | 0 | 5 | 12 | 17 | 24 | 31 | 36 | 41 |
| 6 | 0 | 6 | 14 | 22 | 30 | 36 | 44 | 50 |
| 7 | 0 | 7 | 16 | 25 | 34 | 43 | 52 | 61 |

Now we can do some arithmetic base 8 using the table. All numbers written below are base 8.

$$\begin{array}{r} 51 \\ +\underline{47} \end{array} \qquad\qquad \begin{array}{r} 51 \\ *\underline{47} \end{array}$$

Of course base 2 is simpler! Counting to 15, in groups of 4 we have

$$\begin{array}{l} 0, 1, 10, 11 \\ 100, 101, 110, 111 \\ 1000, 1001, 1010, 1011 \\ 1100, 1101, 1110, 1111 \end{array}$$

The last number is $1111_2 = 8 + 4 + 2 + 1 = 15$.

The addition and multiplication tables are super simple.

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 10 |

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

**Exercise 1:** Convert the base 10 numbers 57 and 235 and 1000 to each base 1,2,4,5,8, and 16. Convert back to base 10 to make sure your anwers are correct.

**Exercise 2:** Convert to base 2: $67AF_{16}$, and $5734_8$. Convert to base 4, 8, and 16: 101110111011

**Exercise 3:** Using the addition and a multiplication table base 8, compute the following.

$$\begin{array}{r} 3742 \\ +\underline{3647} \end{array} \qquad\qquad \begin{array}{r} 452 \\ *\underline{35} \end{array}$$

**Exercise 4:** Let's work base 5 now. First, count to $100_5$ base 5. Then write an addition table and a multiplication table. Then do the following computations.

$$\begin{array}{r} 3142 \\ +\underline{3244} \end{array} \qquad\qquad \begin{array}{r} 412 \\ *\underline{34} \end{array}$$

## 4 Rational and Real Numbers

It takes some work to define exactly what we mean by rational numbers and **much** more work to define exactly what we mean by real numbers.

For our purposes, the set of *rational numbers*, which we write $\mathbb{Q}$, is the set of all fractions $a/b$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. On the rationals, as on $\mathbb{Z}$, we have two operations, $+, *$. This means that $r + s$ and $r * s$ are rational whenever $r$ and $s$ are rational. These operations have the familiar properties below.

- **Commutativity**: Both $+$ and $*$ are commutative. For all rationals $r$ and $s$, $r + s = s + r$ and $r * s = s * r$.
- **Associativity:** Both $+$ and $*$ are associative. For all rationals $r, s, t$, $(r + s) + t = r + (s + t)$ and $(r * s) * t = r * (s * t)$.
- **Identity** Both $+$ and $*$ have identity elements, 0 and 1 respectively. For any rational $r$, $0 + r = r$ and $1 * r = r$.
- **Inverses** Both $+$ and $-$ admit inverses. For any rational $r$, there is a unique rational, which we write $-r$ such that $r + (-r) = 0$. For any nonzero rational $r$, there is a unique rational, which we write $1/r$ such that $r * (1/r) = 1$.
- **Distributivity:** $*$ distributes over $+$. For all real numbers $r, s, t$, $r * (s + t) = r * s + r * t$.

We have a fundamental theorem.

**Theorem 4.1.** *Each nonzero rational number $r$ can be expressed in a unique way as*

$$r = \frac{a}{b} \qquad \textit{where } a \in \mathbb{Z} \textit{ and } b \in \mathbb{N} \textit{ and } \gcd(a, b) = 1.$$

This unique expression for $r$ is called "the lowest terms" for $r$.

For our purposes, the set of *real numbers*, which we write $\mathbb{R}$, is the set of all decimal numbers, including infinite non-repeating decimals. The set of real numbers has two operations $+, *$ satisfying all of the properties that the rationals do.

The *irrational* numbers are the real numbers that aren't rational, that is $\mathbb{R} - \mathbb{Q}$. Some worthwhile things to know about the irrationals are below. The proofs are Level 2.

**Theorem 4.2.** *The negative of an irrational is also irrational.*

**Proof:** By the "additive inverse" property for the rationals, we know that
for all real numbers $r$, if $r$ is rational then $-r$ is rational.
Since $-(-r) = r$ we have
for all real numbers $r$, if $-r$ is rational then $-(-r) = r$ is rational.
Take the contrapositive of this statement.
For all real numbers $r$, if $r$ is not rational then $-r$ is not rational.

**Theorem 4.3.** *The sum of a rational and an irrational is irrational.*

This can be proven by contradiction. Here is another way.

**Proof:** Let $Q(r)$ be the predicate "$r$ is rational." The statement we want to prove is

$$\forall s, t \in \mathbb{R}, (Q(s) \wedge \sim Q(t)) \longrightarrow \sim Q(s+t)$$

We showed that $p \longrightarrow (q \vee r)$ is logically equivalent to $p \wedge \sim q \longrightarrow r$. So the statement we want to prove is equivalent to

$$\forall s, t \in \mathbb{R}, Q(s) \longrightarrow (Q(t) \vee \sim Q(s+t))$$

Applying the same the same trick, this time to $\sim Q(s+t)$, we get the equivalent statement

$$\forall s, t \in \mathbb{R}, Q(s) \wedge Q(s+t) \longrightarrow Q(t)$$

This last statement is true! For real number $s$ and $t$, if $s$ is rational and $s+t$ is rational, then $t = (s+t) - s$ is also rational. Our original statement was equivalent to the last statement, which is true. Thus our original statement is true.

The other important proof to know is the irrationality of $\sqrt{2}$. More generally, we can show

**Theorem 4.4.** *For any prime number $p$, $\sqrt{p}$ is irrational.*

We will do the proof for $\sqrt{2}$ in class. You can also read it in the book. See if you can adapt it to $\sqrt{3}$.