MATH 13150: Freshman Seminar
Unit 16

1. kth roots in mod p arithmetic

In this chapter, we'll learn how to compute kth roots in mod p arithmetic, when p is prime.
The first subtlety is that kth roots don't always exist, or when they exist, there may be more than one. The key point is that when k and p-1 are relatively prime, there is exactly one kth root mod p, and further, there is a systematic way to compute the kth root.

1.1. Some examples.

To begin, let's recall how we think about the kth root of a number a in ordinary arithmetic. The case you may be most familiar with are square roots.
In ordinary arithmetic, we say $a = \sqrt{b}$ if a is a positive number, and $a^2 = b$. This means that
$(\sqrt{a})^2 = a$ if $a \geq 0$ and
$\sqrt{a^2} = a$ if $a \geq 0$.
For example, $\sqrt{16} = 4$ because $4^2 = 16$, and certainly $(\sqrt{16})^2 = 16$.
We can say a is a kth root of b if $a^k = b$. When this happens, we use the notation $\sqrt[k]{b} = a$ to indicate that a is a kth root of b.
It is easy to believe that $(\sqrt[k]{b})^k = b$ and $\sqrt[k]{b^k} = b$, but one needs to be careful. For the first statement, we need to be sure that $\sqrt[k]{b}$ exists for this to make sense. For example, $\sqrt[4]{-16}$ does not exist because a^4 is never negative. For the second statement, we have to require that b is positive, since otherwise, we may have $\sqrt[4]{(-2)^4} = \sqrt[4]{16} = 2$, so $\sqrt[4]{(-2)^4} = \sqrt[4]{2^4} = 2$. But anyway, for us, the thing to remember is that:
$\sqrt[k]{b} = a$ when $a^k = b$, except that sometimes $\sqrt[k]{b}$ does not exist, and sometimes when it exists, there is more than one answer.
For example, 2 and -2 could both be taken to be $\sqrt[4]{16}$, since $2^4 = (-2)^4 = 16$.
In modular arithmetic, we'd like to do the same thing. We set:
NOTION OF KTH ROOT MOD m : A mod m number a is called a kth root of b (mod m) if $a^k \equiv b \pmod{m}$. We write $a \equiv \sqrt[k]{b} \pmod{m}$ when this happens.
As in usual arithmetic, we write $\sqrt{b} \pmod{m}$ in place of $\sqrt[2]{b} \pmod{m}$.
For example, $8^3 \equiv 2 \pmod{15}$, so 8 is a $3rd$ root of 2 in mod 10 arithemtic, and we write $8 \equiv \sqrt[3]{2} \pmod{15}$.
It's useful to look at a table of powers:

Mod 7 table of powers

n	1	2	3	4	5	6	7	8	9	10	11	12
1^n	1	1	1	1	1	1	1	1	1	1	1	1
2^n	2	4	1	2	4	1	2	4	1	2	4	1
3^n	3	2	6	4	5	1	3	2	6	4	5	1
4^n	4	2	1	4	2	1	4	2	1	4	2	1
5^n	5	4	6	2	3	1	5	4	6	2	3	1
6^n	6	1	6	1	6	1	6	1	6	1	6	1

We can use the table to compute $\sqrt[4]{2} \pmod 7$. For this, we look in the 4-column for 2, and we find it in the 2-row and in the 5-row. This means that $2^4 \equiv 2 \pmod 7$ and $5^4 \equiv 2 \pmod 7$, so we can say:
$\sqrt[4]{2} \equiv 2 \pmod 7$ and $\sqrt[4]{2} \equiv 5 \pmod 7$. This means $\sqrt[4]{2} \pmod 7$ is multiply defined, or there are two 4th roots of 2 mod 7.
PROBLEM: Compute $\sqrt[4]{3} \pmod 7$.
To solve this, we look in the 4-column of the table for 3, and we don't find it. In fact, the only entries in the 4-column are $1, 2$ and 4. This means that $\sqrt[4]{3} \pmod 7$ does not exist, since 3 is not $a^4 \pmod 7$. This is like saying that $\sqrt{-9}$ does not exist in ordinary arithmetic (because a negative number like -9 is not the square of a number).
PROBLEM: Compute $\sqrt[5]{2} \pmod 7$.
To solve this, we look in the 5-column of the table for 2 and find it in the 4-row. This means that $4^5 \equiv 2 \pmod 7$, so $\sqrt[5]{2} \equiv \sqrt[5]{4^5} \equiv 4 \pmod 7$, which answers our question.
If we look at the table some more, we see that we can always compute $\sqrt[5]{b} \pmod 7$ for any b:
$1^5 \equiv 1 \pmod 7$, so $\sqrt[5]{1} \equiv 1 \pmod 7$:
$2^5 \equiv 4 \pmod 7$, so $\sqrt[5]{4} \equiv 2 \pmod 7$
$3^5 \equiv 5 \pmod 7$, so $\sqrt[5]{5} \equiv 3 \pmod 7$
$4^5 \equiv 2 \pmod 7$, so $\sqrt[5]{2} \equiv 4 \pmod 7$
$5^5 \equiv 3 \pmod 7$, so $\sqrt[5]{3} \equiv 5 \pmod 7$
$6^5 \equiv 6 \pmod 7$, so $\sqrt[5]{6} \equiv 6 \pmod 7$
So we see that mod 7, there may be one 4th root of a number, and some 4th roots do not exist, while every mod 7 number has exactly one 5th root. This is reflected in the fact that the 4-column has repeated entries and not every mod 7 number appears, while in the 5-column, every mod 7 number appears exactly once.
Let's look at another table of powers.

Mod 11 table of powers

n	1	2	3	4	5	6	7	8	9	10
1^n	1	1	1	1	1	1	1	1	1	1
2^n	2	4	8	5	10	9	7	3	6	1
3^n	3	9	5	4	1	3	9	5	4	1
4^n	4	5	9	3	1	4	5	9	3	1
5^n	5	3	4	9	1	5	3	4	9	1
6^n	6	3	7	9	10	5	8	4	2	1
7^n	7	5	2	3	10	4	6	9	8	1
8^n	8	9	6	4	10	3	2	5	7	1
9^n	9	4	3	5	1	9	4	3	5	1
10^n	10	1	10	1	10	1	10	1	10	1

PROBLEM: How many $\sqrt[4]{3}$ (mod 11) are there? What are they?

SOLUTION: When we look at the 4-column of the table, we see that $4^4 \equiv 7^4 \equiv 3 \pmod{11}$, so 4 and 7 are both $4th$ roots of 3 in mod 11 arithmetic. This solves the problem.

On the other hand, $\sqrt[4]{2}$ (mod 11) does not exist, since 2 does not occur in the 4-column.

PROBLEM: For which k from 1 to 10, does every mod 11 number have a kth root mod 11?

SOLUTION: We look for columns in the mod 11 table of powers so that every mod 11 number occurs. They are $k = 1, 3, 7, 9$. This answers the question.

1.2. **When is there exactly one $\sqrt[k]{b} \pmod{p}$?** We learned in the last section how to find $\sqrt[k]{b} \pmod{p}$ if we have a table in front of us. In this section, we'll learn a general result telling us when there is exactly one $\sqrt[k]{b} \pmod{p}$.

Theorem 1.1. *If* $\gcd(k, p-1) = 1$, *there is exactly one* $\sqrt[k]{b} \pmod{p}$, *while if* $\gcd(k, p-1)$ *is not* 1, *then either there is more than one* $\sqrt[k]{b} \pmod{p}$, *or there is no* kth *root of* b *mod* p. *Further, if* $\gcd(k, p-1) = 1$, *then* $\sqrt[k]{a^k} \equiv a \pmod{p}$.

In the next section, we'll learn a way to compute $\sqrt[k]{b} \pmod{p}$ when $\gcd(k, p-1) = 1$, and this will enable us to explain the theorem. For now, we'll just familiarize ourselves with what the theorem asserts. We'll mainly be interested in computing $\sqrt[k]{b} \pmod{p}$ when $\gcd(k, p-1) = 1$.

EXAMPLE: If $p = 7$, then $p - 1 = 6$. The theorem says that if $\gcd(k, 6) = 1$, then there is exactly one kth root of each mod 7 number. Certainly $\gcd(1, 6) = 1$, and every number has exactly one $1st$ root, and $\gcd(5, 6) = 1$, and every number has exactly one $5th$ root, as we saw above. On the other hand, $\gcd(2, 6) = 2$, so there is no guarantee that every number has exactly one square root. In fact, if we look at the 2-column of mod 7 powers, we see that $1, 2$ and 4 have 2 square roots, but $3, 5$ and 6 do not have square roots. Further, $\gcd(3, 6) = 3$, and 1 and 6 each have three $3rd$ roots, while $2, 3, 4, 5$ do not have $3rd$ roots, since they do not appear in the

3-column. The pattern repeats every 6 numbers, so if $k = 7$ or 11, there is only one kth root mod 7.

EXAMPLE: If $p = 11$, then $p - 1 = 10$, so Theorem 1.1 asserts that there is exactly one kth root of b mod 11 when $\gcd(k, 10) = 1$. The numbers from 1 to 10 so that $\gcd(k, 10) = 1$ are $k = 1, 3, 7, 9$. This agrees with the answer we found in the Problem at the end of the previous section, so the theorem agrees with what we found from the table.

PROBLEM: Is there exactly one $\sqrt[3]{7} \pmod{23}$? Is there exactly one $\sqrt[14]{5} \pmod{23}$?

To solve this, take $p = 23$, so $p-1 = 22$. We compute $\gcd(3, 22) = 1$ and $\gcd(14, 22) = 2$. This means that there is exactly one $\sqrt[3]{7} \pmod{23}$, but there is not exactly one $\sqrt[14]{5} \pmod{23}$. There may be no $\sqrt[14]{5} \pmod{23}$, or there may be more than one. From our point of view, we just think of this as a bad situation where we won't be able to compute the answer easily. Note that the answer has nothing to do with the 7 or 5, but only has to do with the k in $\sqrt[k]{b} \pmod{23}$.

PROBLEM: For which numbers k is there exactly one $\sqrt[k]{2} \pmod{23}$?

The theorem says that $\sqrt[k]{2} \pmod{23}$ is guaranteed to exist only for k such that $\gcd(k, 22) = 1$. The numbers k with this property are:
$1, 3, 5, 7, 9, 13, 15, 17, 19, 21,$
and the pattern repeats every 22 numbers.

1.3. **Computing $\sqrt[k]{b} \pmod{p}$.** In this section, we'll learn a general method for computing $\sqrt[k]{b} \pmod{p}$ when p is prime, p does not divide b, and $\gcd(k, p-1) = 1$. This method does not depend on looking at tables, and works even when p and k are large.

EXAMPLE: Compute $\sqrt[9]{3} \pmod{23}$.

We are taking $k = 9$, $b = 3$, and $p = 23$. Fermat's theorem tells us that:
$3^{22} \equiv 1 \pmod{23}$, and this certainly implies that:
$3^{23} \equiv 3^{22} \cdot 3^1 \equiv 3 \pmod{23}$.
Similarly,
$3^{45} \equiv 3^{2 \cdot 22} \cdot 3^1 \equiv 3 \pmod{23}$.
This second statement enables us to solve the problem. Since $45 = 5 \cdot 9$,
$3^{5 \cdot 9} \equiv 3^{45} \equiv 3 \pmod{23}$, so
$3^{5 \cdot 9} \equiv 3 \pmod{23}$.
Now take the 9th root of each side, which gives,
$\sqrt[9]{3} \equiv \sqrt[9]{3^{5 \cdot 9}} \equiv \sqrt[9]{(3^5)^9} \equiv 3^5 \pmod{23}$.
In the last step, we used the statement $\sqrt[9]{a^9} \equiv a \pmod{23}$, which is the idea behind the notion of kth root, and it is guaranteed by Theorem 1.1. Anyway, we conclude that:
$\sqrt[9]{3} \equiv 3^5 \pmod{23}$.
It remains to compute $3^5 \equiv 13 \pmod{23}$, so
$\sqrt[9]{3} \equiv 13 \pmod{23}$.

You can verify that this is correct by computing $13^9 \equiv 3 \pmod{23}$. When you do these problems, it is a good idea to check your work, because it is easy to make a small mistake somewhere.
The key idea in this was to find a number m so that $m \cdot 9 \equiv 1 \pmod{22}$. We can generalize this example to give the following procedure:

5 STEP PROCEDURE FOR COMPUTING $\sqrt[k]{b} \pmod{p}$ when p is prime, p does not divide b, and $\gcd(k, p-1) = 1$.

STEP 1: Verify that $\gcd(k, p-1) = 1$ and that p does not divide b. Find integers m and s so that

$$m \cdot k + s \cdot (p-1) = 1,$$

using the reverse Euclidean algorithm.
STEP 2: It follows using Fermat's theorem that

$$b^{m \cdot k} \equiv b \pmod{p}.$$

STEP 3: Take the kth root of each side of the last equality to get:

$$b^m \equiv \sqrt[k]{b} \pmod{p}.$$

STEP 4: Compute $c \equiv b^m \pmod{p}$. This is the answer, so $\sqrt[k]{b} \equiv c \pmod{p}$.
STEP 5: Check your answer by computing $c^k \pmod{p}$. If $c^k \equiv b \pmod{p}$, then your answer is correct.

EXAMPLE: Compute $\sqrt[7]{5} \pmod{19}$.

SOLUTION: STEP 1: It is clear that 19 does not divide 5, and not hard to check that $\gcd(7, 18) = 1$. This means we can proceed with the method. We now write 1 as a combination of 7 and 18, using the reverse Euclidean algorithm. The Euclidean algorithm gives:

$18 = 2 \cdot 7 + 4$
$7 = 4 + 3$
$4 = 3 + 1$, so

$1 = 4 - 3 = 3 - (7 - 4) = 2 \cdot 4 - 7$
$1 = 2 \cdot (18 - 2 \cdot 7) - 7 = 2 \cdot 18 - 5 \cdot 7$, so
$1 = 2 \cdot 18 - 5 \cdot 7$. Hence,
$1 \equiv 2 \cdot 18 - 5 \cdot 7 \equiv -5 \cdot 7 \pmod{18}$.

STEP 2: Since $1 \equiv -5 \cdot 7 \pmod{18}$, and $-5 \equiv 13 \pmod{18}$, $1 \equiv 13 \cdot 7 \pmod{18}$. So using the general rule:
$k \equiv r \pmod{p-1}$ implies $a^k \equiv a^r \pmod{p}$ when p does not divide a, we get:
$5 \equiv 5^1 \equiv 5^{13 \cdot 7} \pmod{19}$. Taking 7th roots of each side, we get:

STEP 3: $\sqrt[7]{5} \equiv 5^{13} \pmod{19}$.

STEP 4: Compute $5^{13} \pmod{19}$ through the following steps:
$5^2 \equiv 6 \pmod{19}$
$5^4 \equiv 5^2 \cdot 5^2 \equiv 6 \cdot 6 \equiv 36 \equiv -2 \pmod{19}$

$5^8 \equiv 5^4 \cdot 5^4 \equiv -2 \cdot -2 \equiv 4 \pmod{19}$.
Since $13 = 8 + 4 + 1$, $5^{13} \equiv 5^8 \cdot 5^4 \cdot 5 \equiv 4 \cdot -2 \cdot 5 \equiv -40 \equiv -2 \equiv 17 \pmod{19}$, so $5^{13} \equiv 17 \pmod{19}$.

Conclude that $\sqrt[7]{5} \equiv 5^{13} \equiv 17 \pmod{19}$. This is our answer.

STEP 5: Check our work by verifying that $5 \equiv 17^7 \pmod{19}$. This is easy to check using a calculator, so we have found that:

ANSWER: $\sqrt[7]{5} \equiv 17 \pmod{19}$.

EXAMPLE: Compute $\sqrt[7]{4} \pmod{11}$.

STEP 1: 11 does not divide 4, and $\gcd(7, 10) = 1$. We write 1 as a combination of 7 and 10:
$1 = 3 \cdot 7 - 2 \cdot 10$, so
$1 \equiv 3 \cdot 7 \pmod{11}$.
STEP 2: $4 \equiv 4^{3 \cdot 7} \pmod{11}$.
STEP 3: $\sqrt[7]{4} \equiv 4^3 \pmod{11}$.
STEP 4: Compute $4^3 \equiv 9 \pmod{11}$, so $\sqrt[7]{4} \equiv 9 \pmod{11}$. This is the answer.
STEP 5: Check that $9^7 \equiv 4 \pmod{11}$, which verifies that our answer is correct.
COMMENT: The only step that isn't straightforward from properties of roots is STEP 2. This uses Fermat's theorem. The line of reasoning is:
$1 = 3 \cdot 7 - 2 \cdot 10$, so
$4 \equiv 4^1 \equiv 4^{3 \cdot 7 + -2 \cdot 10} \equiv 4^{3 \cdot 7} \cdot 4^{10 \cdot -2}$, using laws of exponents, so
$4 \equiv 4^{3 \cdot 7} \cdot (4^{10})^{-2} \equiv 4^{3 \cdot 7} \cdot 1^{-2} \equiv 4^{3 \cdot 7} \cdot 1 \equiv 4^{3 \cdot 7}$, where we used Fermat's theorem to conclude that $4^{10} \equiv 1 \pmod{11}$. Some of you may prefer to use the general rule as above, and some of you may prefer to work out the steps (perhpas writing out a little less detail).
Let's now look at another example where the numbers get larger.
EXAMPLE: Compute $\sqrt[5]{11} \pmod{59}$.

SOLUTION: STEP 1: It is clear that 59 does not divide 11, and not hard to check that $\gcd(5, 58) = 1$. We now write 1 as a combination of 5 and 58, using the reverse Euclidean algorithm. The Euclidean algorithm gives:

$58 = 11 \cdot 5 + 3$
$5 = 3 + 2$
$3 = 2 + 1$, so

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$
$1 = 2 \cdot (58 - 11 \cdot 5) - 5 = 2 \cdot 58 - 23 \cdot 5$, so
$1 = 2 \cdot 58 - 23 \cdot 5$.

STEP 2: It follows that $1 \equiv -23 \cdot 5 \pmod{58}$, so since $-23 \equiv 35 \pmod{58}$, $1 \equiv 35 \cdot 5 \pmod{58}$. So using the general rule:
$k \equiv r \pmod{p-1}$ implies $a^k \equiv a^r \pmod{p}$ when p does not divide a, we get:
$11 \equiv 11^{35 \cdot 5} \pmod{59}$. Taking 5th roots of each side, we get:

STEP 3: $\sqrt[5]{11} \equiv 11^{35} \pmod{59}$.

STEP 4: Compute $11^{35} \pmod{59}$ through the following steps:
$11^2 \equiv 3 \pmod{59}$.
$11^4 \equiv 9 \pmod{59}$.
$11^8 \equiv 22 \pmod{59}$.
$11^{16} \equiv 12 \pmod{59}$, (using a calculator)
$11^{32} \equiv 26 \pmod{59}$, so
$11^{35} \equiv 11^{32} \cdot 11^2 \cdot 11 \equiv 26 \cdot 3 \cdot 11 \equiv 32 \pmod{59}$.

We conclude that $\sqrt[5]{11} \equiv 32 \pmod{59}$.
STEP 5: Check that $11 \equiv 32^5 \pmod{59}$. You can do this using a calculator. This confirms that:
ANSWER: $\sqrt[5]{11} \equiv 32 \pmod{59}$.

COMMENT: Although there is nothing conceptually difficult about this example compared to the previous one, the numbers are much larger. Unfortunately, this is a feature of typical modular arithmetic calculations of kth roots, and it is going to get worse when we start working with the RSA algorithm. I'll provide an online modular arithmetic calculator by that stage, which will make these computations easier. You will not be able to use the modular arithmetic calculator on exams, so you should be able to work out the kth root computations when the numbers are smaller, as in the previous examples.

PROBLEM: Does the method outlined in this chapter enable us to compute $\sqrt[7]{12} \pmod{71}$?

SOLUTION: If we do STEP 1, we see that 71 does not divide 12, but $\gcd(7, 70) = 7$, so it is not 1. This means that we will not be able to compute $\sqrt[7]{12} \pmod{71}$ using the method of this chapter. We could still try to find solutions by listing all $7th$ powers mod 71, but this is tedious, even with a modular arithmetic calculator. For you, it will suffice to say that the method does not work.

1.4. **Justification of Theorem 1.1.** We can use the idea from the 5-step procedure to justify the first assertion of Theorem 1.1:

ASSERTION: If $\gcd(k, p-1) = 1$, then there is exactly one $\sqrt[k]{b} \pmod{p}$ for any b not divisible by p.

To justify this assertion, we have to show:
(1) There exists $x \pmod{p}$ so that $x^k \equiv b \pmod{p}$.
(2) If y is a number and $y^k \equiv b \pmod{p}$, then $y \equiv x \pmod{p}$.

For (1), we just use the 5-step procedure. We find integers m, s so that $m \cdot k + s \cdot (p-1) = 1$, and then if $x \equiv b^m \pmod{p}$, then $x^k \equiv 1 \pmod{p}$, so $\sqrt[k]{b} \pmod{p}$ exists. Now suppose $y^k \equiv b \pmod{p}$. Then
$y^{k \cdot m} \equiv (y^k)^m \equiv b^m \pmod{p}$.
But since $k \cdot m \equiv 1 \pmod{p-1}$, it follows that $y^{k \cdot m} \equiv y^1 \equiv y \pmod{p}$, so $y \equiv b^m \equiv x \pmod{p}$, which justifies (2). We used the general rule $t \equiv r \pmod{p}$ implies that $y^t \equiv y^r \pmod{p}$ when p does not divide y. Note that p does not divide y, since if p

did divide y, then $y \equiv 0 \pmod p$, so then $b \equiv y^k \equiv 0^k \equiv 0 \pmod p$, and our b is not divisible by p.

EXERCISES:

(1) Using the mod 11 power table in this Unit, say whether or not the following roots exist in mod 11 arithmetic, and if they exist, find them all.
   (a) $\sqrt[5]{3} \pmod{11}$.
   (b) $\sqrt[7]{4} \pmod{11}$.
   (c) $\sqrt[8]{2} \pmod{11}$.
   (d) $\sqrt[8]{7} \pmod{11}$.

(2) For which of the following kth root problems, does the 5 step method for computing $\sqrt[k]{b} \pmod p$ described in section 3 work? You do not have to compute the kth root.
   (a) $\sqrt[5]{22} \pmod{23}$.
   (b) $\sqrt[7]{13} \pmod{17}$.
   (c) $\sqrt[13]{5} \pmod{53}$.
   (d) $\sqrt[5]{3} \pmod{31}$.

(3) Compute $\sqrt[3]{0} \pmod{41}$ (hint: the method of this unit does not work, but you can do the computation anyway).

(4) Compute $\sqrt[11]{3} \pmod{19}$.

(5) Compute $\sqrt[11]{5} \pmod{19}$.

(6) Compute $\sqrt[7]{3} \pmod{17}$.

(7) Compute $\sqrt[7]{2} \pmod{53}$.

(8) Compute $\sqrt[7]{5} \pmod{61}$.

(9) Compute $\sqrt[17]{13} \pmod{101}$.