

On Inverses

Math 453
Bonus Notes
9/14/07

1. If $\gcd(a, m) = 1$, Then the equation $ax \equiv 1 \pmod m$ has a unique solution, which is written $x \equiv a^{-1} \pmod m$.

2. Since $a \cdot x \equiv x \cdot a = (-a)(-x) = (-x)(-a)$ and $1 \cdot 1 = (-1)(-1)$ we always have:

$(a^{-1})^{-1} \equiv a \pmod m$, $(-a)^{-1} \equiv -a^{-1} \pmod m$, $(-a^{-1})^{-1} \equiv -a \pmod m$
and $1^{-1} \equiv 1 \pmod m$, $(-1)^{-1} \equiv -1 \pmod m$ or $(m-1)^{-1} \equiv (m-1) \pmod m$

3. For large a, m , it is best to use the Euclidean algorithm.
 $\gcd(13, 55) = 1$ because $\begin{matrix} 13 = 13 \\ 55 = 5 \cdot 11 \end{matrix}$) no primes in common.

$55 = 4 \cdot 13 + 3$
 $13 = 4 \cdot 3 + 1$
 $3 = 3 \cdot 1$

$1 = 13 - 4 \cdot 3 = 13 - 4(55 - 4 \cdot 13) = (1 - 4(-4))13 - 4 \cdot 55$
 $= 17 \cdot 13 - 4 \cdot 55 \quad (= 221 - 220)$

Since $17 \cdot 13 = 1 + 4 \cdot 55$, $17 \cdot 13 \equiv 1 \pmod{55}$
and $13^{-1} \equiv 17 \pmod{55}$.

(You can also use The Chinese Remainder Theorem.

$13x \equiv 1 \pmod{55} \Leftrightarrow \begin{matrix} 13x \equiv 1 \pmod{5} \\ 13x \equiv 1 \pmod{11} \end{matrix} \Leftrightarrow \begin{matrix} 13 \equiv 3 \pmod{5} & 3x \equiv 1 \pmod{5} \\ 13 \equiv 2 \pmod{11} & 2x \equiv 1 \pmod{11} \end{matrix}$
 $\Leftrightarrow \begin{matrix} x \equiv 2 \pmod{5} \\ x \equiv 6 \pmod{11} \end{matrix} \Leftrightarrow x \equiv 17 \pmod{55}$
(MISSING STEPS).

4. When $m = p$ is prime, $1 \leq a \leq p-1 \Rightarrow \gcd(a, p) = 1$
and we know that $1^{-1} \pmod p \equiv 1$, $(-1)^{-1} \pmod p \equiv -1$.

We can use the rules of #2 to simplify the calculations.
Worked out on next page for $p = 11, 13, 17$
we try to factor $kp + 1$ for small values of k

$p=11$ $12 \equiv 1 \pmod{11}$, so $2 \cdot 6 \equiv 5 \cdot 7 \equiv 1 \pmod{11}$

(2,6) $2^{-1} \equiv 6 \pmod{11}$ $-2 \equiv 9$ $9^{-1} \equiv 5 \pmod{11}$ (5,9)
 $6^{-1} \equiv 2 \pmod{11}$ $-6 \equiv 5$ $5^{-1} \equiv 9 \pmod{11}$ (check. $9 \cdot 5 = 45 \equiv 1 \pmod{11}$)

(3,4) $3^{-1} \equiv 4 \pmod{11}$ $-3 \equiv 8$ $8^{-1} \equiv 7 \pmod{11}$ (7,8)
 $4^{-1} \equiv 3 \pmod{11}$ $-4 \equiv 7$ $7^{-1} \equiv 8 \pmod{11}$ (check $7 \cdot 8 = 56$)

Since $1^{-1} \equiv 1 \pmod{11}$ and $10^{-1} \equiv 10 \pmod{11}$, we're done.

Compressed: (1) (2,6) (5,9), (3,4), (7,8), (10).

$p=13$ $14 \equiv 1 \pmod{13}$ so $2 \cdot 7 = 14 \equiv 1 \pmod{13}$ (6,11).

(2,7) $2^{-1} \equiv 7 \pmod{13}$ $-2 \equiv 11$ $11^{-1} \equiv 6 \pmod{13}$ $11 \cdot 6 = 65 \equiv 1 \pmod{13}$
 $7^{-1} \equiv 2 \pmod{13}$ $-7 \equiv 6$ $6^{-1} \equiv 11 \pmod{13}$

$14+13=27$ $27 \equiv 1 \pmod{13}$ $3 \cdot 9 \equiv 1 \pmod{13}$ (4,10)

(3,9) $3^{-1} \equiv 9 \pmod{13}$ $-3 \equiv 10$ $10^{-1} \equiv 4 \pmod{13}$ $4 \cdot 10 = 40$
 $9^{-1} \equiv 3 \pmod{13}$ $-9 \equiv 4$ $4^{-1} \equiv 10 \pmod{13}$

At this point 1, 12, 2, 7, 6, 11, 3, 9, 4, 10 uses everything but 5 and 8
 and $5 \cdot 8 = 40 \equiv 1 \pmod{13}$ so $5^{-1} \equiv 8 \pmod{13}$
 $8^{-1} \equiv 5 \pmod{13}$.

Since $-5 \equiv 8$, $-8 \equiv 5$, nothing more can be said.

Compressed (1) (2,7) (6,11), (3,9) (4,10), (5,8) (12)

$p=17$ $18 \equiv 1 \pmod{17}$, so $2 \cdot 9 = 3 \cdot 6 \equiv 1 \pmod{17}$.

(2,9) $2^{-1} \equiv 9 \pmod{17}$ $-2 \equiv 15$ $15^{-1} \equiv 8 \pmod{17}$ (8,15)
 $9^{-1} \equiv 2 \pmod{17}$ $-9 \equiv 8$ $8^{-1} \equiv 15 \pmod{17}$

(3,6) $3^{-1} \equiv 6 \pmod{17}$ $-3 \equiv 14$ $14^{-1} \equiv 11 \pmod{17}$ (14,11)
 $6^{-1} \equiv 3 \pmod{17}$ $-6 \equiv 11$ $11^{-1} \equiv 14 \pmod{17}$

$18+17=35=5 \cdot 7$ $5 \equiv 12$ $12^{-1} \equiv 10 \pmod{17}$ (12,10)
 (5,7) $5^{-1} \equiv 7 \pmod{17}$ $-5 \equiv 12$ $10^{-1} \equiv 12 \pmod{17}$
 $7^{-1} \equiv 5 \pmod{17}$ $-7 \equiv 10$

$35+17=52=4 \cdot 13$ $4^{-1} \equiv 13 \pmod{17}$, $17^{-1} \equiv 4 \pmod{17}$
 and with 1, 16, 2, 9, 8, 15, 3, 6, 14, 11, 5, 7, 12, 10, 13, 4 we have.

Compressed. (1) (2,9) (8,15) (3,6) (14,11), (5,7) (12,10) (16)

Supplemental Math 453 Notes for 9/2/07

1. Suppose p is prime. Fermat's Little Theorem implies that $a^p \equiv a \pmod{p}$ for every integer a .

Corollary

Suppose p is prime and $n > 0$ is a positive integer. Then $a^{1+n(p-1)} \equiv a \pmod{p}$ for every integer a .

Proof.

By induction on n . Base case: $n=1$ $a^{1+(p-1)} = a^p \equiv a \pmod{p}$ by Fermat. Now suppose

$$a^{1+n(p-1)} \equiv a \pmod{p} \text{ for all } a.$$

Multiply the equation $a^p \equiv a \pmod{p}$ by $a^{n(p-1)}$ on both sides to get

$$a^{1+(n+1)p-1} = a^{p+n(p-1)} \equiv a^{1+n(p-1)} \pmod{p}$$

By the inductive hypothesis, $a^{1+n(p-1)} \equiv a \pmod{p}$ and we're done.

2. Euler's Theorem implies that $a^{\phi(100)} \equiv 1 \pmod{100}$ if $\gcd(a, 100) = 1$. Since $\phi(100) = 40$, this gives $a^{40} \equiv 1 \pmod{100}$. We can do better.

Theorem

If $\gcd(a, 100) = 1$, then $a^{20} \equiv 1 \pmod{100}$.

Proof.

Since $\gcd(a, 100) = 1 \iff a \equiv 1 \pmod{100} \iff a \equiv 1 \pmod{4}$ and $a \equiv 1 \pmod{25}$

And $\gcd(a, 100) = 1 \iff \gcd(a, 4) = 1$ and $\gcd(a, 25) = 1$.

By Euler, $\gcd(a, 4) = 1 \implies a^{\phi(4)} = a^2 \equiv 1 \pmod{4} \implies (a^2)^{10} = a^{20} \equiv 1 \pmod{4}$
 and $\gcd(a, 25) = 1 \implies a^{\phi(25)} = a^{20} \equiv 1 \pmod{25}$. Thus, $\gcd(a, 100) = 1$
 implies $a^{20} \equiv 1 \pmod{4}$, $a^{20} \equiv 1 \pmod{25}$, so $a^{20} \equiv 1 \pmod{100}$.

3.

n	3^n
0	1
1	3
2	9
3	27
4	81
5	243
6	729
7	2187
8	6561
9	19683
10	59049
11	177147
12	531441
13	1594323
14	4782969
15	14348907
16	43046721
17	129140163
18	387420489
19	1162261467
20	3486784401

A table illustrating this point, with $a=3$

4. If $n = p_1^{a_1} \dots p_r^{a_r}$, where the p_i 's are different primes,

$$\begin{aligned} \text{Then } \phi(n) &= (p_1^{a_1} - p_1^{a_1-1}) \dots (p_r^{a_r} - p_r^{a_r-1}) \\ &= (p_1-1)p_1^{a_1-1} \cdot (p_2-1)p_2^{a_2-1} \dots (p_r-1)p_r^{a_r-1} \end{aligned}$$

Thus, if $p \mid n$, then $p-1 \mid \phi(n)$ and if $p^a \mid n$, $a \geq 2$, then $p^{a-1} \mid \phi(n)$.

5. If $\phi(n) = 2$ and $p \mid n$, then $p-1 \mid 2 \Rightarrow p-1 \in \{1, 2\}$
 so $p = 2$ or 3 . Since $\phi(n) = 2^1 \cdot 3^0$, we cannot have $2^3 \mid n$ or $3 \mid n$

$$\begin{array}{l} 2^a \quad 3^b \\ \phi(1) = 1 \quad \phi(1) = 1 \\ \phi(2) = 1 \quad \phi(3) = 2 \\ \phi(4) = 2 \end{array}$$

The only way to get a product of 2 out of these columns is: $1 \cdot 3, 2 \cdot 3, 2^2 \cdot 1$

so the solutions to $\phi(n) = 2$ are $n = 3, 6, 4$.

6. If $\phi(n) = 4$ and $p \mid n$, then $p-1 \mid 4 \Rightarrow p-1 \in \{1, 2, 4\}$
 so $p = 2$ or 3 or 5 . Since $\phi(n) = 2^2 \cdot 3^0$, we cannot have $2^4 \mid n, 3^2 \mid n$ or $5^2 \mid n$.

$$\begin{array}{l} n = 2^a \quad 3^b \quad 5^c \\ \phi(1) = 1 \quad \phi(1) = 1 \quad \phi(4) = 1 \\ \phi(2) = 1 \quad \phi(3) = 2 \quad \phi(5) = 4 \\ \phi(2^2) = 2 \\ \phi(2^3) = 4 \end{array}$$

To make the product 4, we first look at c : if $c = 1$, then ϕ of the other factors is 1, so $n = 2^0 \cdot 3^0 \cdot 5^1 = 5$ or $n = 2^1 \cdot 3^0 \cdot 5^1 = 10$.
 Otherwise, $c = 0$. If $b = 1$, then $\phi(3) = 2$ so $\phi(2^a) = 2$ i.e. $n = 2^2 \cdot 3^1 \cdot 5^0 = 4 \cdot 3 = 12$
 Finally, if $b = 0$, then $a = 3$, $n = 2^3 \cdot 3^0 \cdot 5^0 = 8$
 $n = 5, 10, 12, 8$.

7. If $\phi(n) = 6$ and $p \mid n$, then $p-1 \mid 6 \Rightarrow p-1 \in \{1, 2, 3, 6\} \Rightarrow p = 2, 3, 4, 7$. But 4 isn't prime, so $n = 2^a \cdot 3^b \cdot 7^d$, $\phi(n) = 2^1 \cdot 3^1$, so we cannot have $2^3 \mid n, 3^3 \mid n, 7^2 \mid n$

$$\begin{array}{l} n = 2^a \quad 3^b \quad 7^d \\ \phi(1) = 1 \quad \phi(1) = 1 \quad \phi(1) = 1 \\ \phi(2) = 1 \quad \phi(3) = 2 \quad \phi(7) = 6 \\ \phi(2^2) = 2 \quad \phi(3^2) = 6 \end{array}$$

To make the product 6, we need a factor of 3 so either $7 \mid n$ or $3^2 \mid n$. If $7 \mid n$, then $n = 2^0 \cdot 3^0 \cdot 7^1 = 7$ or $n = 2^1 \cdot 3^0 \cdot 7^1$; if $3^2 \mid n$, then $n = 2^0 \cdot 3^2 \cdot 7^0 = 9$ or $n = 2^1 \cdot 3^2 \cdot 7^0 = 18$ $n = 7, 14, 9, 18$

1. Theorem Let $n = p_1^{a_1} \dots p_r^{a_r}$ be given in its prime factorization, and let $M = \text{lcm}(\phi(p_1^{a_1}), \dots, \phi(p_r^{a_r}))$. Then, if $\text{gcd}(a, n) = 1$, we have $a^M \equiv 1 \pmod n$.

Proof.

Because of the prime factorization,

$$(*) \quad a^M \equiv 1 \pmod n \iff \begin{matrix} a^M \equiv 1 \pmod{p_1^{a_1}}, & a^M \equiv 1 \pmod{p_2^{a_2}}, \\ \dots & \dots \\ a^M \equiv 1 \pmod{p_r^{a_r}} \end{matrix}$$

This is the Chinese Remainder Theorem, as $\text{gcd}(p_i^{a_i}, p_j^{a_j}) = 1$, (c.f.)

By Euler's Theorem,

$$a^{\phi(p_i^{a_i})} \equiv 1 \pmod{p_i^{a_i}}$$

and since $\phi(p_i^{a_i}) \mid M$ by the definition of an lcm (!)

$$\left(a^{\phi(p_i^{a_i})} \right)^{\frac{M}{\phi(p_i^{a_i})}} \leftarrow \text{an integer} = a^M \equiv 1^{\frac{M}{\phi(p_i^{a_i})}} \equiv 1 \pmod{p_i^{a_i}}$$

This is true for every i , so (*) implies $a^M \equiv 1 \pmod n$.

Ex 1. $n = 100 = 2^2 \cdot 5^2 \quad \phi(2^2) = (2-1) \cdot 2^1 = 2 \quad \phi(5^2) = (5-1) \cdot 5^1 = 20$

$\text{lcm}(2, 20) = 20$, so

$$\text{gcd}(a, 100) = 1 \implies a^{20} \equiv 1 \pmod{100}$$

Ex 2 $n = 72 = 2^3 \cdot 3^2 \quad \phi(2^3) = (2-1) \cdot 2^2 = 4 \quad \phi(3^2) = (3-1) \cdot 3^1 = 6$

$\text{lcm}(4, 6) = 12$, so

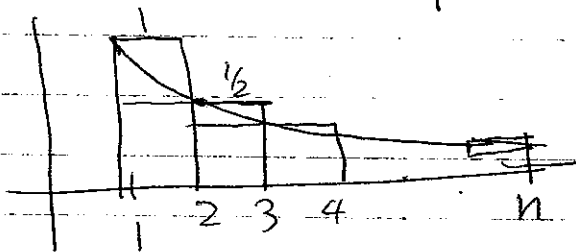
$$\text{gcd}(a, 72) = 1 \implies a^{12} \equiv 1 \pmod{72}$$

Note: $\text{lcm}(\phi(p_1^{a_1}), \dots, \phi(p_r^{a_r}))$ divides the product $\phi(p_1^{a_1}) \cdot \phi(p_r^{a_r}) = \phi(n)$, so this is stronger than Euler's Theorem.

2. An estimate on $d(n)$, the number of divisors of n .

(a) An estimate from calculus.

$$1 + \frac{1}{2} + \dots + \frac{1}{n} \geq \int_1^n \frac{dx}{x} \geq \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n+1}$$

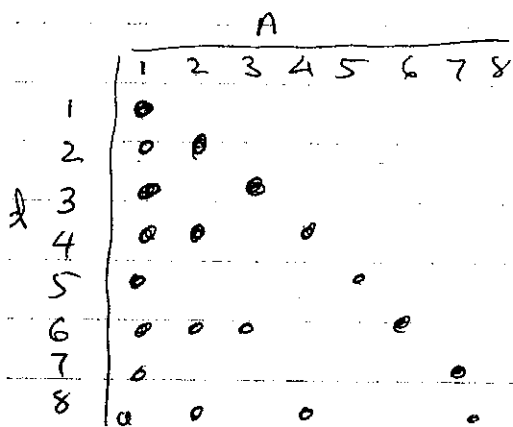


$$\text{so } 1 + \frac{1}{2} + \dots + \frac{1}{n} \geq \log n \geq \frac{1}{2} + \dots + \frac{1}{n+1}$$

$$\begin{aligned} \Rightarrow 1 + \log n &\geq 1 + \frac{1}{2} + \dots + \frac{1}{n+1} \\ \Rightarrow 1 + \log(n-1) &\geq 1 + \frac{1}{2} + \dots + \frac{1}{n} \end{aligned}$$

$$1 + \log(n-1) \geq 1 + \frac{1}{2} + \dots + \frac{1}{n} \geq \log n$$

(b).



$\sum_{n=1}^N d(n)$ is the sum of the divisor

function from 1 to N . It's

counting the dots horizontally (for $N=8$)

if we count the dots vertically,

so that we count the number of times d is a divisor of n , as requested (do

we get $\sum_{d=1}^N \lfloor \frac{N}{d} \rfloor$

Therefore $\sum_{n=1}^N d(n) = \sum_{d=1}^N \lfloor \frac{N}{d} \rfloor$. For any x , $x \geq \lfloor x \rfloor > x-1$

$$\text{so } \sum_{d=1}^N \frac{N}{d} \geq \sum_{n=1}^N d(n) \geq \sum_{d=1}^N \left(\frac{N}{d} - 1 \right) = \left(\sum_{d=1}^N \frac{N}{d} \right) - N \quad \text{Divide by } N.$$

$$\sum_{d=1}^N \frac{1}{d} \geq \frac{1}{N} \sum_{n=1}^N d(n) \geq \left(\sum_{d=1}^N \frac{1}{d} \right) - 1 \geq \log N - 1.$$

As $N \rightarrow \infty$, the "average" number of divisors gets arbitrarily large.

Illustration of Möbius Inversion

Math 453
Extra notes
10/5/07

$$F(n) = \sum_{d|n} f(d) \quad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

As in class: $n=12$, an illustration of the formula in action

$$F(1) = f(1)$$

$$F(2) = f(1) + f(2)$$

$$F(3) = f(1) + \quad + f(3)$$

$$F(4) = f(1) + f(2) \quad + f(4)$$

$$F(6) = f(1) + f(2) + f(3) \quad + f(6)$$

$$F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$$

$$\sum_{d|12} \mu\left(\frac{12}{d}\right) F(d) = \mu(12)F(1) + \mu(6)F(2) + \mu(4)F(3) + \mu(3)F(4) \\ + \mu(2)F(6) + \mu(1)F(12)$$

Recall:

$$\mu(1) = 1$$

$$\mu(p_1 \cdots p_k) = (-1)^k$$

$$\mu(n) = 0 \text{ if } p^2 | n \\ \text{same prime.}$$

$$\mu(1) = 1$$

$$\mu(2) = -1$$

$$\mu(3) = -1$$

$$\mu(6) = (-1)^2 = 1$$

$$\mu(4) = 0 \quad 2^2 | 4$$

$$\mu(12) = 0 \quad 2^2 | 12$$

So we want to look at $0 \cdot F(1) + 1 \cdot F(2) + 0 \cdot F(3) - 1 \cdot F(4) \\ - 1 \cdot F(6) + 1 \cdot F(12)$

$$= F(2) - F(4) - F(6) + F(12)$$

$$= f(1) + f(2) - f(1) - f(2) - f(4) - f(1) - f(2) - f(3) - f(6) \\ + f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$$

$$= f(1)(1 - 1 - 1 + 1) + f(2)(1 - 1 - 1 + 1) + f(3)(-1 + 1) + f(4)(-1 + 1) \\ + f(6)(-1 + 1) + f(12) \cdot 1 = f(12).$$

There are many applications of Möbius inversion in "higher" mathematics; that is, the sort of classes that grad students take