$$f_{p^n}(a) = f_p(f_p(\cdots(a)\cdots)).$$

Since the composition of homomorphisms is a homomorphism (an easy exercise), we have that

$$(a+b)^{p^n} = f_{p^n}(a+b) = f_{p^n}(a) + f_{p^n}(b) = a^{p^n} + b^{p^n}.$$

□

Exercises.

71. Let $m = 15$, then $\lambda(m) = 4$. Verify that for every number a,

$$a^5 \equiv a \pmod{m}.$$

72. Let $m = 41 \cdot 11 = 451$. Verify that

$$11^{\lambda(m)+1} \equiv 11 \pmod{m}.$$

73. Show that $\lambda(m) < \phi(m)$ for every odd composite number m.

74. Find examples of p, q primes >10 so that $\lambda(pq) = p - 1$.

75. Let a, b, c be integers and p a prime. Show that

$$(a+b+c)^p \equiv a^p + b^p + c^p \pmod{p}.$$

Generalize.

76. Find integers a, b so that

$$(a+b)^4 \not\equiv a^4 + b^4 \pmod{4}.$$

77. Show that for all integers a, b and every $n > 0$,

$$(a+b)^n \equiv a^n + b^n \pmod{2}.$$

F. Finding High Powers Modulo *m*

For finding inverses by Euler's theorem and for other applications, we often need to find the least nonnegative residue of a high power of a number modulo m.

For example, one way to find the inverse of 87 modulo 179 is as 87^{177} mod 179.

But if we put 87^{177} into a calculator, it will either choke or give us something like "$1.972\,E+343$", which is useless for discovering that 107 is the inverse of 87 modulo 179.

To find 87^{177} modulo 179, it is helpful to write the exponent in base 2 and then find the result using a sequence of squarings modulo 179. We first find that $179 = 128+32+16+1$. Then we compute

$$\begin{aligned}
&87\\
&87^2 \equiv 51 \pmod{179},\\
&87^4 \equiv 51^2 \equiv 95 \pmod{179},\\
&87^8 \equiv 95^2 \equiv 75 \pmod{179},\\
&87^{16} \equiv 75^2 \equiv 76 \pmod{179},\\
&87^{32} \equiv 76^2 \equiv 48 \pmod{179},\\
&87^{64} \equiv 48^2 \equiv 156 \pmod{179},\\
&87^{128} \equiv 156^2 \equiv 171 \pmod{179}.
\end{aligned}$$

Since $179 = 128+32+16+1$, we have

$$\begin{aligned}
87^{179} &= 87^{128+32+16+1}\\
&= 87^{128}\cdot 87^{32}\cdot 87^{16}\cdot 87\\
&\equiv (171)(48)(76)(87)\\
&\equiv 107 \pmod{179}.
\end{aligned}$$

An efficient way to do the computations is as follows: write the exponent, 177, in base 2: $177 = (10110001)_2$. Then write down that base 2 number with an S inserted in the spaces between adjacent digits:

$$1S0S1S1S0S0S0S1.$$

Now replace each 1 by X and erase each 0, to get

$$XSSXSXSSSSX.$$

Beginning with the number 1, view X and S, from left to right, as operations to compute $a^{177} \pmod{m}$, as follows: X means, multiply the result by a and reduce modulo m; and S means, square the result and reduce modulo m. If we do not reduce modulo m, we would get:

$$\begin{array}{ccccccccccc}
 & & X & & S & & S & & X & & S & \\
1 & \to & a & \to & a^2 & \to & a^4 & \to & a^5 & \to & a^{10} & \\
X & & S & & S & & S & & S & & X & \\
\to a^{11} & \to & a^{22} & \to & a^{44} & \to & a^{88} & \to & a^{176} & \to & a^{177} &
\end{array}$$

If we reduce modulo m at each step, we get the least nonnegative residue of $a^{101} \pmod{m}$ at the end. Thus

$$\begin{aligned}
X:&\ 1\cdot 87 \equiv 87 \pmod{179}\\
S:&\ 87\cdot 87 \equiv 51 \pmod{179}\\
S:&\ 51\cdot 51 \equiv 95 \pmod{179}\\
X:&\ 95\cdot 87 \equiv 31 \pmod{179}\\
S:&\ 31\cdot 31 \equiv 66 \pmod{179}\\
X:&\ 66\cdot 87 \equiv 14 \pmod{179}\\
S:&\ 14\cdot 14 \equiv 17 \pmod{179}\\
S:&\ 17\cdot 17 \equiv 110 \pmod{179}\\
S:&\ 110\cdot 110 \equiv 107 \pmod{179}\\
S:&\ 107\cdot 107 \equiv 172 \pmod{179}\\
X:&\ 172\cdot 87 \equiv 107 \pmod{179}.
\end{aligned}$$

So

$$87^{177} \equiv 107 \pmod{179}.$$

Exercises.

78. Find the least nonnegative residue (mod 34) of 12^{87}.

79. Find the least nonnegative number a congruent to $2^{69} \pmod{71}$. Verify that $2a \equiv 1 \pmod{71}$.

80. Find the least nonnegative number a congruent to $5^{69} \pmod{71}$. Verify that $5a \equiv 1 \pmod{71}$.

81. Find the least nonnegative number a congruent to $3^{340} \pmod{341}$.

82. Find the least nonnegative number a congruent to $5^{1728} \pmod{1729}$.

83. Find the least nonnegative residue (mod 101) of 18^{77}.

84. (i) Find the least nonnegative number a congruent to $2^{1194648} \pmod{1194649}$ Could 1194649 be prime?

(ii) Find the least nonnegative number a congruent to $3^{1194648} \pmod{1194649}$ Is 1194649 prime?

85. Let $m = 252601$. Suppose we discover that

$$\begin{aligned}
3^{126300} &\equiv 67772 \pmod{252601}\\
3^{252600} &\equiv 1 \pmod{252601}
\end{aligned}$$

Is then 252601 prime? composite? Or can we not decide for sure from the information given?

86. Show how to adapt Russian Peasant Arithmetic (Chapter 2, Exercise 29) with multiplication replacing addition and squaring replacing multiplying by 2, to efficiently find a^e and $a^e \bmod m$ for any numbers a, e and m.

G. Modular Multiplication

When we find $a^e \bmod m$ as in Section F, every time we perform an operation (multiplication, squaring), we immediately reduce the result modulo m to bring the result back to a number $<m$. (If we don't, the size of the numbers can become unmanageably large.)

For example, suppose the modulus $m = 179$ and we square 107 to get $107^2 = 11449$. To find its least non-negative residue modulo m, we divide 179 into 11449 and take the remainder.

But long division is the only algorithm in classical arithmetic that is not automatic.

Consider dividing 179 into 11449. We look for the first digit of the quotient. Since 17 is bigger than 11, we can't guess the first digit by dividing the first digit of the divisor into the first digit or two of the dividend. So we start guessing with 9:

$$\begin{aligned} 179 \cdot 9 &= 1611; \\ 179 \cdot 8 &= 1432; \\ 179 \cdot 7 &= 1253; \\ 179 \cdot 6 &= 1074 \end{aligned}$$

and 1074 is less than 1144. So the first digit is 6.

We subtract 10740 from 11449 and get 709. Now we guess the next digit. How many times does 179 go into 709? We try the first digit idea: since 1 goes into 7, 7 times, we start with 7:

$$\begin{aligned} 179 \cdot 7 &= 1253, \\ 179 \cdot 6 &= 1074, \\ 179 \cdot 5 &= 895, \\ 179 \cdot 4 &= 716, \\ 179 \cdot 3 &= 537, \end{aligned}$$

and 537 is less than 709. So the second digit is 3, and the remainder is $709 - 537 = 172$.

Hence $11449 \bmod 179 = 172$, and so $107 \cdot 107 \bmod 179$ is 172.

To find the digits of the quotient, we needed to guess, and trial divide, nine times.

Evidently, we can learn how to do long division by guessing. But for programming a computer, it could be helpful to find a systematic way to find the least non-negative residue of a number without the trial dividing that is part of the long division algorithm.

We present a method, due to P. Montgomery in 1985, which replaces the long division by several multiplications. Here is how it works.

Given the modulus m, we choose a base, or radix $r > m$ such that m is coprime to r, and such that finding the least non-negative residue of any number modulo r is easy. For example, if we are working with numbers written in the usual decimal notation and the modulus m is coprime to 10, then we can choose r to be a power of

10. For then the least non-negative residue of a number is just the rightmost digits of the number.

For example, if $r = 1000$ then 324,554,217 modulo 1000 is 217, while 11449 modulo 1000 is 449.

In our example, if $m = 179$, then we can choose $r = 1000$.

For many applications, such as cryptography, the assumption that the modulus m is coprime to 10 will always hold.

Precomputation. Given the modulus m and the base $r > m$, we first precompute some constants for the algorithm. Since m and r are coprime, we can find numbers r' and m' so that $r'r - m'm = 1$, or

$$r'r = 1 + m'm,$$

where $0 < r' < m$ and $0 < m' < r$. Note that r' is the inverse of r modulo m.

We also find the least non-negative residue w of $r^2 \bmod m$. The constants r', m' and w are used in the algorithm.

The algorithm. Now let b be a number $<mr$. We want to find $b \bmod m$.

We do it in two parts.

For the first part we find $br' \bmod m$, as follows.

First, let $s = bm' \bmod r$. (That, recall, is easy to do.) Then, multiplying by m yields

$$sm = bm'm \pmod{mr},$$

and since $s < r$, then $sm < rm$ and sm is the least non-negative residue of $b'bm$ modulo mr. Then

$$b + sm \equiv b + bm'm = b(1 + m'm) = br'r \pmod{mr},$$

so $b + sm$ is a multiple of r. Divide the congruence

$$b + sm \equiv br'r \pmod{mr}$$

by r (again, easy to do), to get $z = (b + sm)/r$. Then

$$z \equiv br' \bmod m.$$

We also have that

$$z < 2m.$$

To see this, recall that $b < mr$ by assumption, and $sm < mr$. So $rz = b + sm < 2mr$, hence $z < 2m$.

The least non-negative residue c of $br' \bmod m$ is then either z, if $z < m$, or $z - m$, if $m \le z < 2m$.

For the second part of the algorithm, multiply c and w, where w is the least non-negative residue of r^2 modulo m that we precomputed earlier. Then $wc < m^2 < mr$, and

$$wc \equiv r^2 br' \equiv br \pmod{m}.$$

If we then repeat the first part on wc instead of b, we will end up with a number $d < m$ so that

$$d \equiv wcr' \equiv brr' \equiv b \pmod{m},$$

and so d is the least non-negative residue of b modulo m.

In outline, to find $b \bmod m$ for $b < mr$:

- find $s = bm' \bmod r$,
- compute $z = (b + sm)/r$. Then $z < 2m$.
- determine c where $c = z$ if $z < m$ and $c = z - m$ if $z \geq m$.
- find $s' = wcm' \bmod r$,
- compute $z' = (wc + s'm)/r$. Then $z' < 2m$.
- determine d where $d = z'$ if $z' < m$ and $d = z' - m$ if $z' \geq m$.

Then $d = b \bmod m$.

Example 3. Let $m = 179$ and choose the radix $r = 1000$. For the precomputation, we find that $179 \cdot 581 + 1 = 1000 \cdot 104$, and $r^2 = 1000^2 \equiv 106 \pmod{179}$. So

$$r' = 104,$$
$$m' = 581,$$
$$w = 106.$$

For the algorithm itself, let $b = 107 \cdot 107 = 11449$. We want to find b modulo $m = 179$.

First, we find

$$s \equiv bm' = 11449 \cdot 581 \bmod 1000.$$

We can find s efficiently by first reducing $b = 11449 \bmod 1000$ to get 449, then multiplying 449 by $m' = 581$ to get 260869, then reducing 260869 modulo 1000 to get

$$s = 869.$$

Then $sm = 869 \cdot 179 = 155551$, the least non-negative residue of $bm'm$ modulo mr. So

$$\begin{aligned} b + sm &= 11449 + 155551 = 167000 \\ &\equiv b + bm'm = b(1 + m'm) = br'r \pmod{rm} \end{aligned}$$

is a multiple of $r = 1000$. So

$$z = (b + sm)/r = 167000/1000 = 167.$$

Then $z = 167$ satisfies

$$167 \equiv 11449 \cdot 104 = br' \bmod 179.$$

Since $167 < 179$, we have

$$c = 167.$$

Now we multiply $c = 167$ by the least non-negative residue $w = 106$ of r^2 to get

$$wc = 167 \cdot 106 = 17702 \equiv br \pmod{m}.$$

We find $wc \cdot m' = 17702 \cdot 581 = 10284862$, then

$$s' = wcm' \bmod 1000 = 862.$$

Then $s'm = 862 \cdot 179 = 154298$, and

$$\begin{aligned} wc + s'm &= 17702 + 154298 = 172000 \\ &\equiv wc + wcm'm = wc(1 + m'm) = wcr'r \pmod{rm}, \end{aligned}$$

a multiple of $r = 1000$. So

$$z' = 172.$$

Since $172 < 179$, we have

$$d = 172,$$

the least non-negative residue of $b = 11449$ modulo 179.

To sum up, once we set up Montgomery's algorithm for a particular modulus m and radix r by precomputing m', r' and w, the algorithm finds the least non-negative residue of any number $b < mr$, replacing long division by m with five multiplications of numbers $< m$ and five divisions by r. The guessing or trial division that can arise in long division is eliminated.

The Montgomery algorithm has been called the most efficient algorithm available for modular multiplication. It is being built into circuitry designed to do fast modular multiplication of numbers of sizes up to 2^{2048} (numbers of up to 616 digits). We'll see some applications of modular multiplication of large numbers in later chapters.

The original algorithm appeared in Montgomery (1985).

Exercises.

87. Use Montgomery's algorithm to find
(i) $132 \cdot 89 \bmod 179$,
(ii) $167 \cdot 148 \bmod 179$.

88. Set up Montgomery's algorithm for $m = 267$. Use it to find $167 \cdot 239 \bmod 267$.

89. Try this "pick a number" puzzle on a friend:
Pick something you know your friend does at least one day per week. Ask her:
"Write down how many days last week you did [that thing]? Don't show it to me."
Call the secret number m. (m should be a number with $1 \leq m \leq 7$).

Tell her to do the following:

- Take her secret number, add it to 42, call the result t.
- Take the units digit of t, multiply it by 7, take the units digit of the result, multiply that by 7, add the result to t, then divide by 5. Call the result u.
- Then take the units digit of u, multiply it by 7, take the units digit of the result, multiply that by 7, add the result to u, then divide by 10.

Then tell her that the number she computed was the number of days last week she did [that thing].

(i) If she says you're wrong, can you accuse her of making an error in her computations?

(ii) Try to explain to her why it works (if it does!).

(iii) Write up the result of your trial.

90. Make up your own "pick a number" puzzle based on Montgomery's algorithm.