Mathematics of Cryptography

Number Theory

Modular Arithmetic:
Two numbers equivalent mod $n$ if their difference is multiple of $n$
example: 7 and 10 are equivalent mod 3 but not mod 4
7 mod 3 $\equiv$ 10 mod 3 $\equiv$ 13 mod 3 $\equiv$ 16 mod 3 = 1
7 mod 4 = 3 but 10 mod 4 = 2.
Modular Arithmetic: Two numbers equivalent mod $n$ if their difference is multiple of $n$

example: 7 and 10 are equivalent mod 3 but not mod 4
  $7 \mod 3 \equiv 10 \mod 3 \equiv 13 \mod 3 \equiv 16 \mod 3 = 1$
  $7 \mod 4 = 3$ but $10 \mod 4 = 2$.

Is $5643 \mod 123 \equiv 1432 \mod 123$?
Mathematics of Cryptography

Number Theory

Modular Arithmetic:

Two numbers equivalent mod $n$ if their difference is multiple of $n$

example: 7 and 10 are equivalent mod 3 but not mod 4

7 mod 3 $\equiv$ 10 mod 3 $\equiv$ 13 mod 3 $\equiv$ 16 mod 3 = 1
7 mod 4 = 3 but 10 mod 4 = 2.

Is 5643 mod 123 $\equiv$ 1432 mod 123?

$5643 - 1432 = 4211 \equiv u \times 123$ for some integer $u$? Ans: No
Number Theory

Modular Arithmetic:
Two numbers \textbf{equivalent} mod \(n\) if their difference is multiple of \(n\)
example: 7 and 10 are equivalent mod 3 but not mod 4
7 mod 3 \(\equiv\) 10 mod 3 \(\equiv\) 13 mod 3 \(\equiv\) 16 mod 3 = 1
7 mod 4 = 3 but 10 mod 4 = 2.

Is 5643 mod 123 \(\equiv\) 1432 mod 123?
5643 – 1432 = 4211 \(\neq\) \(u\times123\) for some integer \(u\)? Ans: No

Is 5643 mod 123 \(\equiv\) 1830 mod 123?
Number Theory

Modular Arithmetic:
Two numbers equivalent \( \text{mod } n \) if their difference is multiple of \( n \)
example: 7 and 10 are equivalent mod 3 but not mod 4
\[
7 \text{ mod } 3 \equiv 10 \text{ mod } 3 \equiv 13 \text{ mod } 3 \equiv 16 \text{ mod } 3 = 1
\]
\[
7 \text{ mod } 4 = 3 \text{ but } 10 \text{ mod } 4 = 2.
\]

Is 5643 mod 123 \( \equiv \) 1432 mod 123\?
\[
5643 - 1432 = 4211 \neq u \times 123 \text{ for some integer } u? \text{ Ans: No}
\]

Is 5643 mod 123 \( \equiv \) 1830 mod 123\?
\[
5643 - 1830 = 3813 \neq u \times 123 \text{ for some integer } u? \text{ Ans: Yes}
\]
Number Theory

Modular Arithmetic:
Two numbers equivalent mod $n$ if their difference is multiple of $n$
example: 7 and 10 are equivalent mod 3 but not mod 4
$7 \mod 3 \equiv 10 \mod 3 \equiv 13 \mod 3 \equiv 16 \mod 3 = 1$

Greatest Common Divisor:
Largest integer that evenly divides two given numbers
$\gcd(3, 7) = 1; \gcd(294, 385) = 7;$
$294 = 42 \times 7; \ 385 = 55 \times 7;$
Mathematics of Cryptography

Number Theory

Modular Arithmetic:
Two numbers equivalent mod \(n\) if their difference is multiple of \(n\)
example: 7 and 10 are equivalent mod 3 but not mod 4
7 mod 3 \(\equiv\) 10 mod 3 \(\equiv\) 13 mod 3 \(\equiv\) 16 mod 3 \(=\) 1

Greatest Common Divisor:
Largest integer that evenly divides two given numbers
\(\text{gcd}(3, 7) = 1; \text{gcd}(294, 385) = 7;\)
\(294 = 42 \times 7; 385 = 55 \times 7;\)

Given integers \(m, n\), suppose positive integer \(r\) is the smallest
for which there exist integers \(u, v\) such that
\(u \times m + v \times n = r\)
then \(r\) is the greatest common divisor of \(m\) and \(n\).
Number Theory

Modular Arithmetic:
Two numbers equivalent mod $n$ if their difference is multiple of $n$
example: 7 and 10 are equivalent mod 3 but not mod 4
$7 \mod 3 \equiv 10 \mod 3 \equiv 13 \mod 3 \equiv 16 \mod 3 = 1$

Greatest Common Divisor:
Largest integer that evenly divides two given numbers
gcd(3, 7) = 1; gcd(294, 385) = 7;
$294 = 42 \times 7; 385 = 55 \times 7$;

Given integers $m, n$, suppose positive integer $r$ is the smallest for which there exist integers $u, v$ such that
$u \times m + v \times n = r$
then $r$ is the greatest common divisor of $m$ and $n$.

If $p > r$ is common divisor then $u \times m/p + v \times n/p = \text{an integer} = r/p < 1$
Greatest Common Divisor

385
294
Greatest Common Divisor

\[
\frac{385}{294} = 1 \text{ R } 91 \quad 91 = 1 \times 385 - 1 \times 294
\]
Greatest Common Divisor

\[
\frac{385}{294} = 1 \text{ R } 91 \quad \text{In other words we need the gcd of } 91 + 294 \text{ and } 294
\]
Greatest Common Divisor

\[
\frac{385}{294} = 1 \text{ R } 91 \quad \text{In other words we need the gcd of } 91 + 294 \text{ and } 294
\]

But this is the same gcd as for 91 and 294!
Greatest Common Divisor

\[
\frac{385}{294} = 1 \text{ R } 91 
\]

In other words we need the gcd of 91 + 294 and 294
But this is the same gcd as for 91 and 294!

Say \( r \) is the gcd of 385 and 294
Then \( r \) is the smallest integer such that
\[
(91+294)\cdot u + 294\cdot v = r
\]
for some \( u \) and \( v \) integers
Greatest Common Divisor

\[
\begin{array}{c}
\frac{385}{294} = 1 \text{ R } 91 \\
\end{array}
\]

In other words we need the gcd of 91 + 294 and 294

But this is the same gcd as for 91 and 294!

Say \( r \) is the gcd of 385 and 294

Then \( r \) is the smallest integer such that

\[
(91+294)u + 294v = r
\]

for some \( u \) and \( v \) integers

It’s also the smallest integer such that

\[
91u + 294(u+v) = r
\]

Hence \( r \) is the gcd of 91 and 294
Greatest Common Divisor

385
294  \quad 91 = 1 \times 385 - 1 \times 294
294
91
Greatest Common Divisor

385
294
91 = 1\times385 - 1\times294

\[ \frac{294}{91} = 3 \text{ R } 21 \]

21 = 294 - 3(385 - 294) = -3\times385 + 4\times294
Greatest Common Divisor

\[
\begin{align*}
385 & \quad 91 = 1 \times 385 - 1 \times 294 \\
294 & \\
294 & \quad 21 = -3 \times 385 + 4 \times 294 \\
91 & \\
91 & \\
21 &
\end{align*}
\]
Greatest Common Divisor

\[
\begin{align*}
385 & \quad 91 = 1 \times 385 - 1 \times 294 \\
294 & \\
91 & \quad 21 = -3 \times 385 + 4 \times 294 \\
21 & \\
91 & = 4 \text{ R } 7 \\
21 & \quad 7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294
\end{align*}
\]
Greatest Common Divisor

\[
\begin{align*}
385 \\
294 \\
294 \\
91 \\
91 \\
21 \\
7
\end{align*}
\]

\[
7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294
\]
Greatest Common Divisor

385
294
294
91
91
21

7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294

21

\underline{7} = 3 \text{ R } 0
Greatest Common Divisor

385
294
91
294
91
21
7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294

So, the gcd of 385 and 294 is 7
Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$. 
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$.

In other words, find $u$ such that $u \times m + v \times n = 1$ for some $v$. 
Finding Multiplicative Inverses

Find an inverse of \( m \mod n \). That is, a number \( u \) such that \( u \times m = 1 \mod n \).

In other words, find \( u \) such that \( u \times m + v \times n = 1 \) for some \( v \).

Apply previous algorithm (\( \gcd(m,n) \)) to get \( u, v \) but only if \( m \) and \( n \) are relatively prime.
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of \( m \mod n \). That is, a number \( u \) such that \( u \times m = 1 \mod n \).

In other words, find \( u \) such that \( u \times m + v \times n = 1 \) for some \( v \).

Apply previous algorithm (\( \gcd(m,n) \)) to get \( u, v \) but only if \( m \) and \( n \) are relatively prime.

Example:

Inverse of \( 89 \mod 42 \):
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of \( m \) mod \( n \). That is, a number \( u \) such that \( u \times m = 1 \) mod \( n \).

In other words, find \( u \) such that \( u \times m + v \times n = 1 \) for some \( v \).

Apply previous algorithm (gcd(\( m, n \))) to get \( u, v \) but only if \( m \) and \( n \) are relatively prime.

Example:

Inverse of \( 89 \) mod \( 42 \): 
\[ 89 - 2 \times 42 = 5 \]
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$.

In other words, find $u$ such that $u \times m + v \times n = 1$ for some $v$.

Apply previous algorithm ($\gcd(m,n)$) to get $u$, $v$ but only if $m$ and $n$ are relatively prime.

Example:
Inverse of $89 \mod 42$:
$89 - 2 \times 42 \Rightarrow 5 = 1 \times 89 - 2 \times 42$
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$.

In other words, find $u$ such that $u \times m + v \times n = 1$ for some $v$.

Apply previous algorithm ($\gcd(m,n)$) to get $u, v$ but only if $m$ and $n$ are relatively prime.

Example:

Inverse of $89 \mod 42$:

$89 - 2 \times 42 \Rightarrow 5 = 1 \times 89 - 2 \times 42$

$42 - 8 \times 5 = 2$
Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$.

In other words, find $u$ such that $u \times m + v \times n = 1$ for some $v$.

Apply previous algorithm (gcd($m,n$)) to get $u, v$ but only if $m$ and $n$ are relatively prime.

Example:
Inverse of 89 mod 42:

89 - 2×42 $\Rightarrow$ 5 = 1×89 - 2×42

42 - 8×5 $\Rightarrow$ 2 = 1×42 - 8(1×89 - 2×42) = -8×89 + 17×42
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of \( m \) mod \( n \). That is, a number \( u \) such that \( u \times m \equiv 1 \mod n \).

In other words, find \( u \) such that \( u \times m + v \times n = 1 \) for some \( v \).

Apply previous algorithm (gcd(\( m,n \))) to get \( u, v \) but only if \( m \) and \( n \) are relatively prime.

Example:

Inverse of \( 89 \mod 42 \):

\[
89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42 \\
42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42 \\
5 - 2 \times 2 = 1
\]
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of \( m \mod n \). That is, a number \( u \) such that \( u\times m = 1 \mod n \).

In other words, find \( u \) such that \( u\times m + v\times n = 1 \) for some \( v \).

Apply previous algorithm (\( \gcd(m,n) \)) to get \( u, v \) but only if \( m \) and \( n \) are relatively prime.

Example:

Inverse of \( 89 \mod 42 \):

\[
\begin{align*}
89 - 2\times42 & \rightarrow 5 = 1\times89 - 2\times42 \\
42 - 8\times5 & \rightarrow 2 = 1\times42 - 8(1\times89 - 2\times42) = -8\times89 + 17\times42 \\
5 - 2\times2 & \rightarrow 1 = 1\times89 - 2\times42 - 2(-8\times89 + 17\times42) = 17\times89 - 36\times42
\end{align*}
\]
Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \mod n$. That is, a number $u$ such that $u \times m = 1 \mod n$.

In other words, find $u$ such that $u \times m + v \times n = 1$ for some $v$.

Apply previous algorithm ($\gcd(m,n)$) to get $u$, $v$ but only if $m$ and $n$ are relatively prime.

Example:

Inverse of $89 \mod 42$:

$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$

$42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42$

$5 - 2 \times 2 \rightarrow 1 = 1 \times 89 - 2 \times 42 - 2(-8 \times 89 + 17 \times 42) = 17 \times 89 - 36 \times 42$

Conclusion: 17 is the inverse of 89 mod 42!

Look at the applet
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If $p$ is prime and $0 < a < p$, then $a^{p-1} \equiv 1 \mod p$

Ex: $3^{(5-1)} = 81 = 1 \mod 5$
$36^{(29-1)} = 37711171281396032013366321198900157303750656$
$= 1 \mod 29$

Look at the applet
Mathematics of Cryptography

Modulo arithmetic – Fermat’s Little Theorem

If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

Ex: $3^{(5-1)} = 81 = 1 \mod 5$

$36^{(29-1)} = 377111712813960320133660321198900157303750656$

$= 1 \mod 29$

Every number $a$ has either 2 square roots ($\sqrt{a}, -\sqrt{a}$) or 0 square roots
Solve $x^2 = a \mod p$ where $p$ is a prime number.
If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

*Ex:* $3^{(5-1)} = 81 = 1 \mod 5$
$36^{(29-1)} = 37711171281396032013366321198900157303750656$
$= 1 \mod 29$

Every number $a$ has either 2 square roots ($\sqrt{a}$, $-\sqrt{a}$) or 0 square roots

Solve $x^2 = a \mod p$ where $p$ is a prime number.

1. $p \mod 4$ can be either 1 or 3 – suppose it is 3
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} \equiv 1 \pmod{p} \)

**Ex:** \( 3^{(5-1)} = 81 = 1 \pmod{5} \)
\( 36^{(29-1)} = 37711171281396032013366321198900157303750656 \)
\( = 1 \pmod{29} \)

Every number \( a \) has either 2 square roots (\( \sqrt{a} \), \( -\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \pmod{p} \) where \( p \) is a prime number.

1. \( p \pmod{4} \) can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} \equiv 1 \mod p \)

*Ex*: \( 3^{(5-1)} = 81 = 1 \mod 5 \)

\( 36^{(29-1)} = 37711171281396032013366321198900157303750656 \)

\( = 1 \mod 29 \)

Every number \( a \) has either 2 square roots (\( \sqrt{a}, -\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \mod p \) where \( p \) is a prime number.

1. \( p \mod 4 \) can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
3. but \( a^{(p-1)/2} = 1 \mod p \);
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} = 1 \mod p \)

\( Ex: \ 3^{(5-1)} = 81 = 1 \mod 5 \)

\( 36^{(29-1)} = 37711171281396032013366321198900157303750656 \)

\( = 1 \mod 29 \)

Every number \( a \) has either 2 square roots (\( \sqrt{a}, -\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \mod p \) where \( p \) is a prime number.

1. \( p \mod 4 \) can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
3. but \( a^{(p-1)/2} = 1 \mod p; \ a^{(4t+3-1)/2} = 1 \mod p; \)
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} = 1 \mod p \)

\[ 3^{(5-1)} = 81 = 1 \mod 5 \]
\[ 36^{(29-1)} = 37711171281396032013366321198900157303750656 \]
\[ = 1 \mod 29 \]

Every number \( a \) has either 2 square roots (\( \sqrt{a}, -\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \mod p \) where \( p \) is a prime number.

1. \( p \) mod 4 can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
3. but \( a^{(p-1)/2} = 1 \mod p \); \( a^{(4t+3-1)/2} = 1 \mod p \); \( a^{2t+1} = 1 \mod p \)
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

$Ex$: $3^{(5-1)} = 81 = 1 \mod 5$

$36^{(29-1)} = 37711171281396032013366321198900157303750656$

$= 1 \mod 29$

Every number $a$ has either 2 square roots ($\sqrt{a}$, $-\sqrt{a}$) or 0 square roots

Solve $x^2 = a \mod p$ where $p$ is a prime number.

1. \( p \mod 4 \) can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where $t$ is some positive integer
3. but $a^{(p-1)/2} = 1 \mod p$; $a^{(4t+3-1)/2} = 1 \mod p$; $a^{2t+1} = 1 \mod p$
   $a^{2t+2} = a \mod p$;
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} \equiv 1 \pmod{p} \)

Ex: \( 3^{(5-1)} = 81 = 1 \pmod{5} \)
\[ 36^{(29-1)} = 37711171281396032013366321198900157303750656 \]
\[ = 1 \pmod{29} \]

Every number \( a \) has either 2 square roots (\( \sqrt{a} \), \(-\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \pmod{p} \) where \( p \) is a prime number.

1. \( p \pmod{4} \) can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
3. but \( a^{(p-1)/2} = 1 \pmod{p} \); \( a^{(4t+3-1)/2} = 1 \pmod{p} \); \( a^{2t+1} = 1 \pmod{p} \)
\[ a^{2t+2} = a \pmod{p} \); \( a^{2(t+1)} = a \pmod{p} \);
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

*Ex:* $3^{(5-1)} = 81 = 1 \mod 5$
$36^{(29-1)} = 37711171281396032013366321198900157303750656$
$= 1 \mod 29$

Every number $a$ has either 2 square roots ($\sqrt{a}$, $-\sqrt{a}$) or 0 square roots

Solve $x^2 = a \mod p$ where $p$ is a prime number.

1. $p \mod 4$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where $t$ is some positive integer
3. but $a^{(p-1)/2} = 1 \mod p$; $a^{(4t+3-1)/2} = 1 \mod p$; $a^{2t+1} = 1 \mod p$
   $a^{2t+2} = a \mod p$; $a^{2(t+1)} = a \mod p$; $(a^{t+1})^2 = a \mod p$
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} = 1 \) mod \( p \)

Ex: \( 3^{(5-1)} = 81 = 1 \) mod 5
\( 36^{(29-1)} = 37711171281396032013366321198900157303750656 \)
\( = 1 \) mod 29

Every number \( a \) has either 2 square roots \((\sqrt{a}, -\sqrt{a})\) or 0 square roots

Solve \( x^2 = a \) mod \( p \) where \( p \) is a prime number.

1. \( p \) mod 4 can be either 1 or 3 – suppose it is 3
2. then \( p = 4t + 3 \) where \( t \) is some positive integer
3. but \( a^{(p-1)/2} = 1 \) mod \( p \); \( a^{(4t+3-1)/2} = 1 \) mod \( p \); \( a^{2t+1} = 1 \) mod \( p \)
   \( a^{2t+2} = a \) mod \( p \); \( a^{2(t+1)} = a \) mod \( p \); \( (a^{t+1})^2 = a \) mod \( p \)
4. so, if \( p = 4t + 3 \), then find the \( t \), the square root of \( a \) is \( a^{t+1} \)
Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If \( p \) is prime and \( 0 < a < p \), then \( a^{p-1} \equiv 1 \mod p \)

\( \text{Ex: } 3^{(5-1)} = 81 = 1 \mod 5 \)

\( 36^{(29-1)} = 37711171281396032013366321198900157303750656 \)

\( = 1 \mod 29 \)

Every number \( a \) has either 2 square roots (\( \sqrt{a}, -\sqrt{a} \)) or 0 square roots

Solve \( x^2 = a \mod p \) where \( p \) is a prime number.

1. \( p \mod 4 \) can be either 1 or 3 – suppose it is 3
2. \( \text{then } p = 4t + 3 \) where \( t \) is some positive integer
3. \( \text{but } a^{(p-1)/2} = 1 \mod p; \ a^{(4t+3-1)/2} = 1 \mod p; \ a^{2t+1} = 1 \mod p \)
   \( a^{2t+2} = a \mod p; \ a^{2(t+1)} = a \mod p; \ (a^{t+1})^2 = a \mod p \)
4. \( \text{so, if } p = 4t + 3, \text{ then find the } t, \text{ the square root of } a \text{ is } a^{t+1} \)

example: \( p=19 = 4*4+3, \text{ so } t=4. \quad \text{Suppose } a \text{ is 7} \)

\( \sqrt{7} \mod 19 = 7^5 \mod 19 = 11 \mod 19 \)

check: \( 121 \mod 19 = 7 \mod 19 \)
Finding a prime

Probability that a random number $p$ is prime: $1/\ln(p)$

For 100 digit number this is $1/230$. 
Finding a prime

Probability that a random number $p$ is prime: $1/\ln(p)$

For 100 digit number this is 1/230.

But how to test for being prime?
Mathematics of Cryptography

Finding a prime

Probability that a random number $p$ is prime: $1/\ln(p)$

For 100 digit number this is 1/230.

But how to test for being prime?

If $p$ is prime and $0 < a < p$, then $a^{p-1} \equiv 1 \mod p$
Finding a prime

Probability that a random number $p$ is prime: $1/\ln(p)$

For 100 digit number this is $1/230$.

But how to test for being prime?

If $p$ is prime and $0 < a < p$, then $a^{p-1} \equiv 1 \mod p$

$Pr(p$ isn't prime but $a^{p-1} \equiv 1 \mod p$) is small
Mathematics of Cryptography

Finding a prime

Probability that a random number $p$ is prime: $\frac{1}{\ln(p)}$

For 100 digit number this is $1/230$.

But how to test for being prime?

If $p$ is prime and $0 < a < p$, then $a^{p-1} \equiv 1 \pmod{p}$

$Pr(p \text{ isn't prime but } a^{p-1} \equiv 1 \pmod{p})$ is small

However, the time it takes to compute $a^{p-1}$ is high but can be reduced to a feasible amount of computation using the following theorem
If \( p \) is prime, the only square roots of 1 mod \( p \) are 1 and -1 mod \( p \).

Let \( x \) other than 1 or -1 be a square root of 1 mod \( p \). Then \( x^2 = 1 \) mod \( p \).

Or, \((x-1)(x+1) = 0 \) mod \( p \).

This means the product is divisible by prime \( p \).
By Euclid's lemma \( p \) divides at least one of \((x-1)\) or \((x+1)\).
Therefore, divide out one of \((x-1)\) or \((x+1)\)
In what's left either \((x-1) = 0 \) mod \( p \) so \( x \) is 1 or \((x+1) = 0 \) mod \( p \) so \( x \) is -1.
Finding a prime

Can always express a number $p-1$ as $2^b c$ for some odd number $c$ where $p$ is prime.

Ex: $428 = 2^2 \cdot 107$

Here is the $2^b$

$110101100$

Here is the odd number

Note: $(a^x)^3 = (a^{2x})^2 = (a^{4x})^2 = a^{8x}$ so $\sqrt[3]{\sqrt[2]{\sqrt[2]{(a^x)^3}}} = a^x$
Finding a prime

We can always express a number $a^{p-1}$ as $a^{2^b c}$ for some odd number $c$ where $p$ is prime.

We can compute $a^{p-1} \mod p$ by computing $a^c \mod p$ and squaring the result up to $b$ times.

If $a^c = 1 \mod p$ then $a^{p-1} = 1 \mod p$ and we are done because the square root of $1 \mod p$ is $1 \mod p$ and the square root of that is $1 \mod p$ and so on.

If $a^c \neq 1 \mod p$ then repeatedly square until either getting $a^{2^r c} = -1 \mod p$ for some $r < b$ or not. If $-1 \mod p$ is obtained, $p$ is likely prime because from 2 slides back $\sqrt{a^{p-1}}$ is either $-1$ or $1$, and $1$ is taken care of above. If $-1 \mod p$ is not obtained by squaring, then $p$ cannot be prime because $\sqrt{a^{p-1} = 1 \mod p}$ is not 1 or $-1$. 

Finding a prime
Finding a prime

Example:

Show $11^{12} = 11^{3 \times 2^2} = 1 \mod 13$

$11^3 \mod 13 = 1331 \mod 13 = 5 \rightarrow$ continue

$5^2 \mod 13 = 25 \mod 13 = 12 = -1 \mod 13 \rightarrow$ done
Mathematics of Cryptography

Finding a prime

Example:
Show $11^{12} = 11^{3 \cdot 2^2} = 1 \mod 13$

$11^3 \mod 13 = 1331 \mod 13 = 5 \rightarrow \text{continue}$

$5^2 \mod 13 = 25 \mod 13 = 12 = -1 \mod 13 \rightarrow \text{done}$

Example:
Show $11^{20} = 11^{5 \cdot 2^2} \neq 1 \mod 21$

$11^5 \mod 21 = 161051 \mod 21 = 2 \rightarrow \text{continue}$

$2^2 \mod 21 = 4 \mod 21 = 4 \rightarrow \text{continue}$

$4^2 \mod 21 = 16 \mod 21 = 16 \rightarrow \text{stop (no more 0s and never got to 1)}$
Mathematics of Cryptography

Finding a prime

Second approach to understanding why.

By Fermat's Little Theorem, if $p$ is prime, $a^{2^b c}$ is $1 \mod p$

From 3 slides back, taking the square root of $a^{2^b c}$ gives $1$ or $-1 \mod p$. The square root of $-1 \mod p$ may be a number that is not $1$ or $-1 \mod p$ (ex: try $p = 17$), but the square root of $1$ will still be $1$. Hence repeatedly taking square roots until reaching $a^c$ may always return $1$s or may return a $-1 \mod p$ at some point followed by numbers that are not $1$ or $-1 \mod p$.

Therefore, if $p$ is prime then either $a^c = 1 \mod p$

or for some $r < b$, $a^{2^r c} = -1 \mod p$. 
Choose a random odd integer $p$ to test.
Calculate $b = \# \text{ times } 2 \text{ divides } p-1$.

Calculate $m$ such that $p = 1 + 2^b m$.

Choose a random integer $a$ such that $0 < a < p$.

If $a^m \equiv 1 \mod p \quad \| \quad a^{2^j m} \equiv -1 \mod p$, for some $0 \leq j \leq b-1$, then $p$ passes the test. A prime will pass the test for all $a$. 
Mathematics of Cryptography

Finding a prime – here is an algorithm sketch

Choose a random odd integer \( p \) to test.
Calculate \( b = \# \) times 2 divides \( p-1 \).

Calculate \( m \) such that \( p = 1 + 2^b \, m \).

Choose a random integer \( a \) such that \( 0 < a < p \).

If \( a^m \equiv 1 \mod p \) \| \( a^{2^j \, m} \equiv -1 \mod p \), for some \( 0 \leq j \leq b-1 \),
then \( p \) passes the test. A prime will pass the test for all \( a \).

A non prime number passes the test for at most 1/4 of all possible \( a \).

So, repeat \( N \) times and probability of error is \((1/4)^N \).

Look at the applet
Mathematics of Cryptography

Finding a prime – importance to RSA

Choose $e$ first, then find $p$ and $q$ so $(p-1)$ and $(q-1)$ are relatively prime to $e$

RSA is no less secure if $e$ is always the same and small

Popular values for $e$ are 3 and 65537

For $e = 3$, though, must pad message or else ciphertext = plaintext

Choose $p \equiv 2 \mod 3$ so $p-1 = 1 \mod 3$ so $p$ is relatively prime to $e$

So, choose random odd number, multiply by 3 and add 2, then test for primality
Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?
Mathematics of Cryptography

Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

Application: An army general about 2000 years ago sent by messenger a note to the emperor telling how many troops he had. But the number was encrypted in the following way:
- dividing 602 by 3 gives a remainder of 2
- dividing 602 by 5 gives a remainder of 2
- dividing 602 by 7 gives a remainder of 0
- dividing 602 by 11 gives a remainder of 8

So the message is: 2,2,0,8

It turns out that by the Chinese Remainder Theorem (CRT) it is possible to uniquely determine the number of troops provided all the divisions were by relatively prime numbers.
Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

Application:
An old Chinese woman on the way to the market came upon a horse and rider. The horse stepped on her basket and crushed the eggs in her basket. The rider offered to pay for the broken eggs and asked how many eggs were in the basket. She did not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?
Chinese Remainder Theorem

If the prime factorization of $n$ is $n_1 \times n_2 \times \ldots \times n_k$ then the system of equations:

\[
x \mod n_1 = a_1 \quad x = a_1 \mod n_1
\]
\[
x \mod n_2 = a_2 \quad x = a_2 \mod n_2
\]
\[
x \mod n_3 = a_3 \quad x = a_3 \mod n_3
\]
\[\ldots \ldots \ldots \]
\[
x \mod n_k = a_k \quad x = a_k \mod n_k
\]

has a unique solution $x$ given any $a_1, a_2, \ldots, a_k$ where $x < n$. 
Mathematics of Cryptography

Chinese Remainder Theorem

Why?

Define \( n^i = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k \)

This means, for each \( 1 \leq i \leq k \), there is an \( r_i \) and \( s_i \) such that

\[
r_i n_i + s_i n^i = 1
\]

and \( r_i \) and \( s_i \) can be found using the gcd algorithm.

**Note:** since \( s_i n^i = 1 \mod n_i \), \( (n^i)^{-1} = s_i \mod n_i \)

Since \( n^i \) contains all \( n_j \) as factors except for \( n_i \) it is evenly divisible by all but \( n_i \).

Then \( s_i n^i = 0 \mod n_j \) for all \( i \neq j \) and

\[
s_i n^i = 1 \mod n_i
\]
Mathematics of Cryptography

Chinese Remainder Theorem

Why?

The solution is

\[ x = \sum_{i=1}^{k} a_i \cdot s_i \cdot n_i \mod n_1 n_2 \ldots n_k \]

Therefore, as a check

\[ x \mod n_1 = a_1 \times 1 + a_2 \times 0 + a_3 \times 0 + \ldots + a_k \times 0 = a_1 \]
\[ x \mod n_2 = a_1 \times 0 + a_2 \times 1 + a_3 \times 0 + \ldots + a_k \times 0 = a_2 \]
\[ x \mod n_3 = a_1 \times 0 + a_2 \times 0 + a_3 \times 1 + \ldots + a_k \times 0 = a_3 \]

... 
\[ x \mod n_k = a_1 \times 0 + a_2 \times 0 + a_3 \times 0 + \ldots + a_k \times 1 = a_k \]
Mathematics of Cryptography

Chinese Remainder Theorem

\[
x \mod n_1 = a_1 \quad x \equiv a_1 \mod n_1
\]

\[
x \mod n_2 = a_2 \quad x \equiv a_2 \mod n_2
\]

\[
x \mod n_3 = a_3 \quad x \equiv a_3 \mod n_3
\]

\[...
\]

\[
x \mod n_k = a_k \quad x \equiv a_k \mod n_k
\]

has a unique solution \(x\) given any \(a_1, a_2, \ldots, a_k\) where \(x < n_1n_2 \ldots n_k\)
Mathematics of Cryptography

Chinese Remainder Theorem

\[ x \mod n_1 = a_1 \quad x \equiv a_1 \mod n_1 \]
\[ x \mod n_2 = a_2 \quad x \equiv a_2 \mod n_2 \]
\[ x \mod n_3 = a_3 \quad x \equiv a_3 \mod n_3 \]

\[ \ldots \quad \ldots \]
\[ x \mod n_k = a_k \quad x \equiv a_k \mod n_k \]

Return to the original problem:
divide \( x \) by 3 and get a remainder of 2 \( a_1 = 2 \quad n_1 = 3 \)
divide \( x \) by 5 and get a remainder of 3 \( a_2 = 3 \quad n_2 = 5 \)
divide \( x \) by 7 and get a remainder of 2 \( a_3 = 2 \quad n_3 = 7 \)

What is the value of \( x \) that is no greater than \( 3 \times 5 \times 7 \)?
Mathematics of Cryptography

Chinese Remainder Theorem

\[
x \mod n_1 = a_1 \quad x \equiv a_1 \mod n_1
\]
\[
x \mod n_2 = a_2 \quad x \equiv a_2 \mod n_2
\]
\[
x \mod n_3 = a_3 \quad x \equiv a_3 \mod n_3
\]

...                           ...

\[
x \mod n_k = a_k \quad x \equiv a_k \mod n_k
\]

Return to the original problem:

divide \( x \) by 3 and get a remainder of 2 \( a_1 = 2 \quad n_1 = 3 \)
divide \( x \) by 5 and get a remainder of 3 \( a_2 = 3 \quad n_2 = 5 \)
divide \( x \) by 7 and get a remainder of 2 \( a_3 = 2 \quad n_3 = 7 \)

What is the value of \( x \) that is no greater than \( 3 \times 5 \times 7 \)?

Inverses of: \( 5 \times 7 \mod 3 = 2 \quad 3 \times 7 \mod 5 = 1 \quad 3 \times 5 \mod 7 = 1 \)
Mathematics of Cryptography

Chinese Remainder Theorem

\[
\begin{align*}
x \mod n_1 &= a_1 \quad & x &\equiv a_1 \mod n_1 \\
x \mod n_2 &= a_2 \quad & x &\equiv a_2 \mod n_2 \\
x \mod n_3 &= a_3 \quad & x &\equiv a_3 \mod n_3 \\
\cdots \quad & \cdots \quad & \cdots \\
x \mod n_k &= a_k \quad & x &\equiv a_k \mod n_k 
\end{align*}
\]

Return to the original problem:

divide \( x \) by 3 and get a remainder of 2 \( a_1 = 2 \quad n_1 = 3 \)

divide \( x \) by 5 and get a remainder of 3 \( a_2 = 3 \quad n_2 = 5 \)

divide \( x \) by 7 and get a remainder of 2 \( a_3 = 2 \quad n_3 = 7 \)

What is the value of \( x \) that is no greater than \( 3 \times 5 \times 7 \)?

Inverses of: \( 5 \times 7 \mod 3 = 2 \quad 3 \times 7 \mod 5 = 1 \quad 3 \times 5 \mod 7 = 1 \)

\[
x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \mod 3 \times 5 \times 7 = 23 \ (128, 233, \ldots)
\]
Chinese Remainder Theorem

Second problem:

\[ x = 1 \mod 2 \implies x = 2t + 1 \]
\[ x = 1 \mod 3 \implies x = 3p + 1 \]
\[ x = 1 \mod 4 \implies x = 4r + 1 \]
\[ x = 1 \mod 5 \implies x = 5s + 1 \]
\[ x = 1 \mod 6 \implies x = 6q + 1 \]
\[ x = 0 \mod 7 \implies x = 7w \]
Mathematics of Cryptography

Chinese Remainder Theorem

Second problem: Whoops! not a prime factorization

\[ x = 1 \mod 2 \implies x = 2t + 1 \]
\[ x = 1 \mod 3 \implies x = 3p + 1 \]
\[ x = 1 \mod 4 \implies x = 4r + 1 \]
\[ x = 1 \mod 5 \implies x = 5s + 1 \]
\[ x = 1 \mod 6 \implies x = 6q + 1 \]
\[ x = 0 \mod 7 \implies x = 7w \]

so, \( 2t = 3p = 4r = 5s = 6q \)
from last two \( q = v \times 5 \) and \( s = v \times 6 \)
but \( r = 3q/2 \) so \( q = v \times 2 \times 5 \) and \( s = v \times 2 \times 6 \) making \( r = v \times 3 \times 5 \)
also \( p = 2q = v \times 4 \times 5 \)
and \( t = 2r = v \times 30 \)
so \( x = 60v + 1; n = 7w \)
\( 7w = 60v + 1 \)
Immediate consequence:

Suppose everyone's RSA public key $e$ part is 3. Consider the same message sent to three people. These are:

$$c[1] = m^3 \mod n[1]$$
$$c[2] = m^3 \mod n[2]$$
$$c[3] = m^3 \mod n[3]$$

By the Chinese Remainder Theorem

One can compute $m^3 \mod n[1] \times n[2] \times n[3]$

Since $m$ is smaller than any of the $n[i]$, $m^3$ is known and taking the cube root finds $m$. 
Mathematics of Cryptography

\[ Z^n \]

All numbers less than \( n \) that are relatively prime with \( n \)

Examples: \( Z^{10} = \{ 1, 3, 7, 9 \} \); \( Z^{15} = \{ 1, 2, 4, 7, 8, 11, 13, 14 \} \)

If numbers \( a, b \) are members of \( Z^n \) then so is \( a \times b \mod n \).

Examples: \( 4 \times 11 \mod 15 = 44 \mod 15 = 14; \)
\( 13 \times 14 \mod 15 = 182 \mod 15 = 2. \)
Mathematics of Cryptography

\[ Z^*n \]

All numbers less than \( n \) that are relatively prime with \( n \)

Examples: \( Z^*10 = \{ 1, 3, 7, 9 \} \); \( Z^*15 = \{ 1, 2, 4, 7, 8, 11, 13, 14 \} \)

If numbers \( a, b \) are members of \( Z^*n \) then so is \( a \times b \mod n \).

Examples: \( 4 \times 11 \mod 15 = 44 \mod 15 = 14; \)
\( 13 \times 14 \mod 15 = 182 \mod 15 = 2. \)

Why?

Since \( a \) and \( b \) are relatively prime to \( n \) there must be integers \( u, v \) s.t.
\( u \times a + v \times n = 1 \) and \( w \times b + x \times n = 1. \)
Mathematics of Cryptography

$\mathbb{Z}^*_n$

All numbers less than $n$ that are relatively prime with $n$

Examples: $\mathbb{Z}^*_{10} = \{1, 3, 7, 9\}$; $\mathbb{Z}^*_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

If numbers $a, b$ are members of $\mathbb{Z}^*_n$ then so is $a \times b \mod n$.

Examples: $4 \times 11 \mod 15 = 44 \mod 15 = 14$;

$13 \times 14 \mod 15 = 182 \mod 15 = 2$.

Why?

Since $a$ and $b$ are relatively prime to $n$ there must be integers s.t.

$u \times a + v \times n = 1$ and $w \times b + x \times n = 1$.

Multiply both equations:

$(u \times w) \times a \times b + (u \times x \times a + v \times w \times b + x \times v \times n) \times n = 1$

Hence $a \times b$ is relatively prime to $n$. 
Run applet ZstarN

1. All of the numbers in the $\mathbb{Z}^* n$ row are unique and they all appear uniquely in the $\text{res}$ row.

2. Every number in $\mathbb{Z}^* n$ must have an inverse since 1 must always appear in both rows as implied by the above. For example, if $n$ is 19, the inverse of 9 is found by clicking on the 9 in the $\mathbb{Z}^* n$ row and locating the 1 in the $\text{res}$ row. The number directly above the 1 is 17. Hence, 17 is the inverse of 9 mod 19.

3. The number in the button below the clicked button is the square of the number in the clicked button. Hence the square root of a number, if it exists, may be obtained by clicking buttons until the desired number appears in the $\text{res}$ row beneath the clicked button. The number above that one is its square root.
Mathematics of Cryptography

$\mathbb{Z}^*n$

**Run applet ZstarN**

4. If $n$ is prime, half the numbers of $\mathbb{Z}^*n$ have square roots, the others have no square roots.

5. The two square roots of a number that has square roots are at the same offset from either end of the top row. Hence, for $n=19$, the square root of 1 is 1 and 18, the square root of 4 is 2 and 17, the square root of 9 is 3 and 16 and so on.

6. $n-1 \mod n$ is also $-1 \mod n$. Hence, if $n$ is prime, each square root is $-1$ times the other.
Run applet Z

1. Select a number from the menu, call it \( n \). The set of all numbers that are prime relative to \( n \) appears in a row that is labeled \( \mathbb{Z}^*n \). Select one of the numbers, call it \( a \). Compute \( a^{n-1} \) by clicking on the Multiply button until the count \( n-1 \) is reached. The answer in the result field should be 1.

2. If \( n \) is prime there is a number in \( \mathbb{Z}^*n \), called a generator and denoted \( g \), such that \( g^i, 1 \leq i < n \), is unique, and an element of \( \mathbb{Z}^*n \) and \( g^{n-1} \) is 1. For a generator the result: field will not display 1 until the count is \( n-1 \). A generator for \( n = 19 \) is 10.
Run applet Zmult

1. Select a number from the menu, call it \( n \). The set of all numbers that are prime relative to \( n \) appears in a row that is labeled \( \mathbb{Z}^*n \). Compute the product of all numbers in \( \mathbb{Z}^*n \mod n \) by clicking the Multiply button repeatedly until no more changes take place.

2. Observe if \( n \) is prime; the number in the result: field is \( n-1 \) when finished.
Euler's Totient Function:

Defined: \( \phi(n) \) is number of elements in \( Z^*n \).

Example: \( \phi(7) = 6 \) (\( \{1,2,3,4,5,6\} \)) ; \( \phi(10) = 4 \) (\( \{1,3,7,9\} \))

Suppose \( n = p \times q \) and \( p \) and \( q \) are relatively prime

Example: \( \phi(70) \):

\( \{1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69\} \)

\( \phi(70) = \phi(7)\phi(10) = 24. \)

Why?
Euler's Totient Function:

Defined: \( \phi(n) \) is number of elements in \( \mathbb{Z}^*n \).

Example: \( \phi(7) = 6 \) (\( \{1, 2, 3, 4, 5, 6\} \)) ; \( \phi(10) = 4 \) (\( \{1, 3, 7, 9\} \))

Suppose \( n = p \times q \) and \( p \) and \( q \) are relatively prime

Example: \( \phi(70) \):

\[
\{ 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69 \}
\]

\( \phi(70) = \phi(7)\phi(10) = 24 \).

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number \( m \) and

\[
m_p = m \mod p \quad 1 = 29 \mod 7 \quad 4 = 39 \mod 7
\]

\[
m_q = m \mod q \quad 9 = 29 \mod 10 \quad 9 = 39 \mod 10
\]
Euler's Totient Function:

Defined: \( \phi(n) \) is number of elements in \( Z^*n \).

Example: \( \phi(7) = 6 (\{1,2,3,4,5,6\}) \); \( \phi(10) = 4 (\{1,3,7,9\}) \)

Suppose \( n = p \times q \) and \( p \) and \( q \) are relatively prime

Example: \( \phi(70) \):

\[
\{ 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69 \}
\]

\( \phi(70) = \phi(7)\phi(10) = 24. \)

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number \( m \) and

\[
m_p = m \mod p
\]

\[
m_q = m \mod q
\]

If \( m \) is relatively prime to \( pq \), then there are integers \( u,v \), such that

\( um + vpq = 1. \)
Euler's Totient Function:

Substituting \( m = m_p + kp \) gives

\[ um_p + (uk + vq)p = 1 \]

so \( m_p \) is relatively prime to \( p \). Same for \( m_q \) and \( q \).

Therefore, \( m \) in \( \mathbb{Z}^*_{pq} \) means \( m_p \) is in \( \mathbb{Z}^*_{p} \) and \( m_q \) is in \( \mathbb{Z}^*_{q} \).

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number \( m \) and

\[
\begin{align*}
m_p &= m \mod p \\
m_q &= m \mod q
\end{align*}
\]

If \( m \) is relatively prime to \( pq \), then there are integers \( u,v \), such that

\[ um + vpq = 1. \]
Mathematics of Cryptography

Euler's Totient Function:

Substituting $m = m_p + kp$ gives

$$um_p + (uk + vq)p = 1$$

so $m_p$ is relatively prime to $p$. Same for $m_q$ and $q$.

Therefore, $m$ in $\mathbb{Z}^*pq$ means $m_p$ is in $\mathbb{Z}^*p$ and $m_q$ is in $\mathbb{Z}^*q$.

Similar tricks can be used to show that $m_q$ in $\mathbb{Z}^*q$ and $m_p$ in $\mathbb{Z}^*p$ imply $m$ in $\mathbb{Z}^*pq$.

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number $m$ and

$$m_p = m \mod p$$

$$m_q = m \mod q$$

If $m$ is relatively prime to $pq$, then there are integers $u,v$, such that

$$um + vpq = 1.$$
Euler's Theorem:

For all \( a \) in \( \mathbb{Z}^*n \), \( a^{\phi(n)} = 1 \mod n \).

Why?

By example: suppose \( n = 10, \ a = 3 \). Multiply all elements of \( \mathbb{Z}^*n = \{ 1, 3, 7, 9 \} \) to get \( x = 189 \). But \( x \mod 10 = 9 \) which is an element of \( \mathbb{Z}^*n \). The inverse of \( x \) is 9.
Euler's Theorem:

For all $a$ in $\mathbb{Z}^*n$, $a^{\phi(n)} = 1 \mod n$.

Why?

By example: suppose $n = 10$, $a = 3$. Multiply all elements of $\mathbb{Z}^*n = \{1, 3, 7, 9\}$ to get $x = 189$. But $x \mod 10 = 9$ which is an element of $\mathbb{Z}^*n$. The inverse of $x$ is 9.

Multiply all elements of $\mathbb{Z}^*n$ by 3 and multiply all those numbers:

$$3 \times 1 \times (3 \times 3) \times (3 \times 7) \times (3 \times 9) = 3^{\phi(n)} \times x$$

But $3 \times 1 = 3$, $3 \times 3 = 9$, $3 \times 7 = 1$, $3 \times 9 = 7$ (all mod 10)

Hence $a^{\phi(n)} \times x = x \mod n$.

So, $a^{\phi(n)} = 1 \mod n$
Euler's Theorem:

For all $a$ in $\mathbb{Z}^*_n$, and any non-negative integer $k$, $a^{(k \times \phi(n) + 1)} = a \mod n$.

Why?
Euler's Theorem:

For all $a$ in $\mathbb{Z}^*n$, and any non-neg int $k$, $a^{(k \times \phi(n)+1)} = a \mod n$.

Why? $a^{(k \times \phi(n)+1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$
Euler's Theorem:

For all $a$ in $\mathbb{Z}^*n$, and any non-neg int $k$, $a^{(k\times\phi(n)+1)} = a \mod n$.

Why? $a^{(k\times\phi(n)+1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all $a$ and any non-neg int $k$, $a^{(k\times\phi(n)+1)} = a \mod n$, if $n = p \times q$, $p$ and $q$ are prime then $\phi(n) = (p-1) \times (q-1)$
Mathematics of Cryptography

Euler's Theorem:

For all $a$ in $\mathbb{Z}^*n$, and any non-neg int $k$, $a^{(k \times \phi(n) + 1)} = a \mod n$.

Why? $a^{(k \times \phi(n) + 1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all $a$ and any non-neg int $k$, $a^{(k \times \phi(n) + 1)} = a \mod n$, if $n = p \times q$, $p$ and $q$ are prime then $\phi(n) = (p-1) \times (q-1)$

Why?
Mathematics of Cryptography

Euler's Theorem:

For all $a$ in $Z^*n$, and any non-neg int $k$, $a^{(k \times \phi(n)+1)} = a \mod n$.

Why? $a^{(k \times \phi(n)+1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all $a$ and any non-neg int $k$, $a^{(k \times \phi(n)+1)} = a \mod n$, if $n = p \times q$, $p$ and $q$ are prime then $\phi(n) = (p-1) \times (q-1)$

Why? Only interesting case: $a$ is a multiple of $p$ or $q$.

Suppose $a$ is a multiple of $q$.

Since $a$ is relatively prime to $p$, $a^{\phi(p)} = 1 \mod p$.

Since $\phi(n) = \phi(p) \times \phi(q)$, (mod $p$) $a^{(k \times \phi(n)+1)} = (a^{\phi(p) \times \phi(q)})^k \times a = 1^{(k \times \phi(n))} \times a = a \mod p$ and $a=0 \mod q$ so $a^{(k \times \phi(n)+1)} = 0 = a \mod q$.

By CRT $a^{(k \times \phi(n)+1)} = a \mod n$. 
RSA:

\[ n = p \times q \]

\[ \phi(n) = (p-1) \times (q-1) \]

\( e \) – relatively prime to \( \phi(n) \)

\( d \) – such that \( e \times d - 1 \) divisible by \( \phi(n) \)

hence \( (e \times d - 1) / \phi(n) = k \), a positive integer

so \( e \times d = k \times \phi(n) + 1 \)

therefore \( m^{e \times d} = m^{k \times \phi(n) + 1} = m \mod n \)