Try it

Solve the equation $7y \equiv 3 \pmod{26}$

What do we need to find?
The multiplicative inverse of $7 \pmod{26}$

An application of all of this modular arithmetic

Amazon chooses random 512-bit (or 1024-bit) prime numbers $p, q$ and an exponent $e$ (often about 60,000).

Amazon calculates $n = pq$. They tell your computer $(n, e)$ (not $p, q$)

You want to send Amazon your credit card number $a$.

You compute $C = a^e \pmod{n}$ and send Amazon $C$.

Amazon computes $d$, the multiplicative inverse of $e \pmod{(p-1)(q-1)}$

Amazon finds $C^d \pmod{n}$

Fact: $a = C^d \pmod{n}$ as long as $0 < a < n$ and $p \nmid a$ and $q \nmid a$
Let’s build a faster algorithm.

Fast exponentiation – simple case. What if $e$ is exactly $2^{16}$?

```java
int total = 1;
for(int i = 0; i < e; i++){
    total = a * total % n;
}
```

Instead:

```java
int total = a;
for(int i = 0; i < log(e); i++){
    total = total^2 % n;
}
```

Fast Exponentiation Algorithm

What if $e$ isn’t exactly a power of 2?

Step 1: Write $e$ in binary.

Step 2: Find $a^c \mod n$ for $c$ every power of 2 up to $e$.

Step 3: calculate $a^e$ by multiplying $a^c$ for all $c$ where binary expansion of $e$ had a 1.