Things we have believed about equality since Euclid:
1) $x = x$;
2) If $x = y$ then $y = x$;
3) If $x = y$ and $y = z$ then $x = z$.

Here are some theorems about congruence mod m, for $m \in \mathbb{Z}_{\geq 1}$.

Theorem 7.17. Say $m \in \mathbb{Z}_{\geq 1}$ and $a, b, c \in \mathbb{Z}$.
1) $a \equiv a \bmod m$;
2) If $a \equiv b \bmod m$ then $b \equiv a \bmod m$;
3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

"congruence mod m behaves in a similar way to equality".

Theorem 7.17. Say $m \in \mathbb{Z}_{\geq 1}$ and $a, b, c \in \mathbb{Z}$.

1) $a \equiv a \bmod m$;
2) If $a \equiv b \bmod m$ then $b \equiv a \bmod m$;
3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

Proof.

1) Unfolding the definition of $\equiv$ we see that what we actually have to prove is that $m \mid (a - a)$, or in other words: there exists an integer k such that $mk = (a - a)$. Set $k = 0$; this clearly works.

2) Unfolding the definitions, our assumption is that there exists an integer j such that $a - b = mj$, and our goal is to prove that there exists an integer k such that $b - a = mk$. Setting $k = -j$ does the job.

3) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

This time, our assumptions are that there are integers i and j wuth $a - b = mi$ and $b - c = mj$. Our goal is to find an integer k such that $a - c = mk$. But

$$a - c = (a - b) + (b - c) = mi + mj = m(i + j),$$

so $k = i + j$ works.

Are these proofs 100 percent watertight?

YES. (Click here to see proofs in Lean – wait until it stops saying “running”. Issues with firefox.)

Here is another fact about equality.

If $a = s$ and $b = t$, then $a + b = s + t$. Similarly $a - b = s - t$ and $ab = st$.

Theorem 7.18. Say $m \in \mathbb{Z}_{\geq 1}$. Say $a, b, s, t \in \mathbb{Z}$ and $a \equiv s \bmod m$ and $b \equiv t \bmod m$. Then

(1) $a + b \equiv s + t \bmod m$;
(2) $a - b \equiv s - t \bmod m$;
(3) $ab \equiv st \bmod m$.

Proof. Our assumptions imply that there exists integers j and k such that $a - s = jm$ and $b - t = km$.
(1) It suffices to prove that $(a + b) - (s + t)$ is a multiple of m. But $(a + b) - (s + t) = (a - s) + (b - t) = (j + k)m$.
(2) Try it yourself! $(a - b) - (s - t) = (a - s) - (b - t) = (j - k)m$.
(3) Try it yourself!
$ab - st = a(b - t) + at - at + (a - s)t = akm + jmt = m(ak + jt)$, so $ab - st$ is a multiple of m.

$\square$

We just proved $a \equiv s$ and $b \equiv t$ implied $a + b \equiv s + t$ and $ab \equiv st$. How do we now prove this?

Corollary 7.19 If $m \in \mathbb{Z}_{\geq 1}$, $n \in \mathbb{Z}_{\geq 0}$, and $x_1, x_2, x_3, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are all integers, such that for all $1 \leq i \leq n$ we have $x_i \equiv y_i$ mod m. Then $\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} y_i$ and $\prod_{i=1}^{n} x_i \equiv \prod_{i=1}^{n} y_i$.

Proof. Induction on n.

$\square$

Corollary 7.20 If $m \in \mathbb{Z}_{\geq 1}$ and $n \in \mathbb{Z}_{\geq 0}$, and if $a, b \in \mathbb{Z}$ with $a \equiv b$ mod m, then $a^n \equiv b^n$ mod m.

Proof. Induction on n.

$\square$

Happy? What is 0^0? What does 0^0 need to be in order to make this proof work? $m^0 = 1$ so 0^0 had better be 1.

Let's use the previous few lemmas to do some example calculations which would be a pain to do on a calculator.

Examples. Let $N = 7^{41}$.
What's the remainder when you divide N by 6? By 8? By 11?

Well, $7 \equiv 1 \bmod 6$, so $7^{41} \equiv 1^{41} \equiv 1 \bmod 6$, so the remainder after dividing 7^{41} by 6 is 1.

Modulo 8 we need to dig a little deeper. We see that $7^2 = 49 \equiv 1 \bmod 8$, so $7^{41} = (7^2)^{20} \times 7 \equiv 1^{20} \times 7 \bmod 8$, which is congruent to 7 mod 8, so the remainder when N is divided by 8 is 7. Another way of doing this one: $7 \equiv -1 \bmod 8$, so $7^{41} \equiv (-1)^{41} \equiv -1 \equiv 7 \bmod 8$.

Modulo 11 we need to work even harder (but see later, when we've done Fermat's Little Theorem). Modulo 11 we have $7^2 = 49 \equiv 5 \bmod 11$, so $7^4 \equiv 5^2 = 25 \equiv 3 \bmod 11$, so $7^5 \equiv 3 \times 7 = 21 \equiv -1 \bmod 11$, so $7^{10} \equiv (-1)^2 \equiv 1 \bmod 11$. Hence $7^{40} \equiv 1 \bmod 11$, and so $7^{41} \equiv 1 \times 7 \equiv 7 \bmod 11$.

The rule of 3.

We give a simple method for computing the remainder when a large number is divided by 3.

First note that $10 \equiv 1 \mod 3$. Hence $10^i \equiv 1 \mod 3$ for all $i \in \mathbb{Z}_{\geq 0}$. So if we have a non-negative integer $M = \sum_{i=0}^{n} a_i 10^i$ with a_i all "digits" ($0 \leq a_i \leq 9$), then

$$M = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \mod 3.$$

Hence, for example,
$12345 \equiv 1 + 2 + 3 + 4 + 5 = 15 \equiv 1 + 5 = 6 \equiv 0 \mod 3$, and hence 12345 is a multiple of 3.

The rule of 4.

We give a simple method for computing the remainder when a large number is divided by 4.

First note that $10^2 \equiv 0 \bmod 4$. Hence for all $i \geq 2$ we have $10^i = 10^{i-2} \times 10^2 \equiv 0 \bmod 4$. So if we have anumber $M = \sum_{i=0}^{n} a_i 10^i$ with a_i all “digits” $(0 \leq a_i \leq 9)$, then

$$M = \sum_{i=0}^{n} a_i 10^i \equiv a_0 + 10a_1 \mod 4.$$

Hence, for example, $12345 \equiv 45 \bmod 4$, and hence 12345 leaves remainder 1 after division by 4.

The rule of 11.

We give a simple method for computing the remainder when a large number is divided by 11.

First note that $10 \equiv (-1) \bmod 11$. Hence $10^i \equiv (-1)^i \bmod 11$. So if we have a number $M = \sum_{i=0}^{n} a_i 10^i$ with a_i all "digits" $(0 \leq a_i \leq 9)$, then

$$M = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i (-1)^i \mod 11.$$

Hence, for example, $12345 \equiv 5 - 4 + 3 - 2 + 1 \equiv 3 \bmod 11$, and hence 12345 leaves remainder 3 when divided by 11.

The rule of 37.

We give a fairly simple method for computing the remainder when a large number is divided by 37.

First note that $37 \times 27 = 999$, so $10^3 \equiv 1 \mod 37$. Hence $10^{3n} \equiv 1 \mod 37$. So we can break a number into pieces of size 3 and add them up.
For example, $M = 1002003004005$ modulo 37 – we rewrite as 1 002 003 004 005 and the remainder when dividing M by 37 is $1 + 2 + 3 + 4 + 5 = 15$.

Example. Prove that if n is any integer, then $n^3 - n$ is a multiple of 3.

Well, we know by division and remainder (lemma 7.16) that there exists some integer r with $0 \leq r \leq 2$ such that $n \equiv r \bmod 3$. And then $n^3 - n \equiv r^3 - r \bmod 3$ (why?) (Theorems 7.18 and 7.20), so to check that $n^3 - n$ is always a multiple of 3, we just need to check it for $n = 0, 1, 2$, which is easy.

The question about 7^{41} modulo 11 was a bit of a pain. We can get a less painful solution if we use Fermat's Little Theorem. Fermat's Little Theorem will also give us another proof of the example above, because it implies that $n^3 \equiv n \bmod 3$.

Fermat's Little Theorem.

Not to be confused with Fermat's Last Theorem, Fermat's Little Theorem says this:

Theorem 7.21. If $a \in \mathbb{Z}$ and $p \in \mathbb{Z}_{>1}$ is a prime number, then
(i) $a^p \equiv a \bmod p$; and
(ii) if furthermore $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

Application: we can compute 7^{41} modulo 11 rather more easily now. For Fermat's Little Theorem tells us that $7^{10} \equiv 1 \bmod 11$, and hence $7^{40} \equiv 1^4 \equiv 1 \bmod 11$, so $7^{41} \equiv 7 \bmod 11$.

Before we start the proof, I will prove that (i) implies (ii) and that (ii) implies (i). To put it another way, I will show that (i) and (ii) are *logically equivalent*. The advantage of doing this is that we only have to prove one of them, and we can choose which one.

Theorem 7.21 (Fermat's Little Theorem.) If $a \in \mathbb{Z}$ and $p \in \mathbb{Z}_{>1}$ is a prime number, then
(i) $a^p \equiv a \bmod p$; and
(ii) if furthermore $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

Proof that (i) $\implies$ (ii). Say $a \in \mathbb{Z}$ and p is prime with $p \nmid a$. Assume (i) is true. Then $p \mid a^p - a$. Hence $p \mid a(a^{p-1} - 1)$. Now Corollary 7.12 said $p \mid bc \implies p \mid b \vee p \mid c$. But by assumption $p \nmid a$. Hence $p \mid a^{p-1} - 1$. And hence $a^{p-1} \equiv 1 \bmod p$, as required.
Proof that (ii) implies (i). If $a \in \mathbb{Z}$ then either $p \mid a$ or $p \nmid a$. If $p \mid a$ then $a \equiv 0 \bmod p$, and $a^p \equiv 0^p \equiv 0 \bmod p$. Hence $a^p \equiv a \bmod p$ in this case. If however $p \nmid a$ then by (ii) we know $a^{p-1} \equiv 1 \bmod p$. Multiplying both sides by a we deduce $a^p \equiv a \bmod p$ in this case too.

Conclusion so far: parts (i) and (ii) are equivalent, so we only need to prove one of them. If you had done M1P2 already, I could say "here's a proof of (ii): the non-zero integers mod p are a group of order $p - 1$, and the the order of the element divides the order of the group by Lagrange's theorem, so done. I could even tell you about how $\mathrm{hcf}(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \bmod n$, the Fermat–Euler theorem, and how the proof is just the same.

But M1F is before M1P2, so we have to do it in a slightly more long-winded way.

But first we need

Lemma 7.22 If p is prime and $0 < i < p$ then $p \mid \binom{p}{i}$.

Proof. We know from Proposition 5.3 that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Hence $p! = \binom{p}{i} i!(p-i)!$. Now certainly $p \mid p!$. However if $i < p$ then $i!$ is the product of a bunch of numbers between 1 and $p-1$, and because p is prime and p divides none of these, p does not divide their product either, by Corollary 7.12. So $i < p \implies p \nmid i!$. Similarly $i > 0 \implies p \nmid (p-i)!$. So, because $p \mid \binom{p}{i} i!(p-i)!$, we must have $p \mid \binom{p}{i}$.

$\square$

Proof of 7.21. We have seen that we just need to prove the first part, namely $a^p \equiv a \bmod p$.
By replacing a by its remainder after division by p, we see that we only need to prove it for $0 \leq a \leq p-1$. In fact we prove it for all $a \geq 0$, by induction on a, using the binomial theorem.

Base case : $0^p \equiv 0 \bmod p$: this is fine.

Inductive step: say $d^p \equiv d \bmod p$. Then $(1+d)^p = \sum_{i=0}^{p} \binom{p}{i} d^i$.
Modulo p, most of these terms vanish, by the previous lemma. More precisely, we deduce $(1+d)^p \equiv 1 + d^p \bmod p$. By the inductive hypothesis, $d^p \equiv d \bmod p$. Hence
$(1+d)^p \equiv 1 + d \bmod p$. This finishes the proof of the inductive step, and hence the proof of the theorem.

$\square$