Review. Fermat's little theorem

Corollary 71. For any prime p and any integer a, we have $a^p \equiv a \pmod{p}$.

A freshman's dream. In particular, $(x+y)^p \equiv x^p + y^p \pmod{p}$, for any integers x, y and any prime p.
[This follows from two applications of Fermat's little theorem: $(x+y)^p \equiv x+y \equiv x^p + y^p \pmod{p}$]

Example 72. Compute $407^{7249} \pmod{101}$.

Solution. First, $407^{7249} \equiv 3^{7249} \pmod{101}$. Then, using Fermat, $3^{7249} \equiv 3^{49} \pmod{101}$.
We then use binary exponentiation:
$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, $3^{32} \equiv 16^2 \equiv 54$, all modulo 101
Since $49 = (110001)_2 = 2^0 + 2^4 + 2^5$, we have $3^{49} = 3^{32} \cdot 3^{16} \cdot 3^1 \equiv 54 \cdot 16 \cdot 3 = 2592 \equiv 67 \pmod{101}$.
In conclusion, $407^{7249} \equiv 67 \pmod{101}$.

Example 73. (extra) Using binary exponentiation, compute $5^{49} \pmod{105}$.

Solution. Recall that $49 = (110001)_2 = 2^0 + 2^4 + 2^5$.
$5^1 = 5$, $5^2 = 25$, $5^4 = 25^2 = 625 \equiv -5$, $5^8 \equiv (-5)^2 = 25$, $5^{16} \equiv 25^2 \equiv -5$, $5^{32} \equiv (-5)^2 = 25$
Hence, $5^{49} = 5^{32} \cdot 5^{16} \cdot 5^1 \equiv 25 \cdot (-5) \cdot 5 \equiv 5$.

9 Using Sage as a fancy calculator

Any serious number theory applications, such as those in cryptography, involve computations that need to be done by a machine. Let us see how to use the open-source computer algebra system **Sage** to do basic computations for us.

Sage is freely available at `sagemath.org`. Instead of installing it locally (it's huge!) we can conveniently use it in the cloud at `cocalc.com` from any browser.
Sage is built as a **Python** library, so any Python code is valid. For starters, we will use it as a fancy calculator.

Example 74. Let's start with some basics.

```
Sage] 17 % 12
```
5
```
Sage] (1 + 5) % 2  # don't forget the brackets
```
0
```
Sage] inverse_mod(17, 23)
```
19
```
Sage] xgcd(17, 23)
```
$(1, -4, 3)$
```
Sage] -4*17 + 3*23
```
1

Example 75. Why is the following bad?

```
Sage] 3^1003 % 101
```

```
27
```

The reason is that this computes 3^{1003} first, and then reduces that huge number modulo 101:

```
Sage] 3^1003
```

```
3569591212598177919604229201330789788106639488430800052695284994212437212836103228760\
1014473966417673025563997815559723610675773716716710620364253581964749198745746080354660\
1704706398904182050714408540803174892687110481591021823549827662286672460340211243666\
8093879692989497704687200501870715649428827356779624172512220217218361672427543129732160\
8010229102922713154530775386398517183447789526555113958789446315044211288493307759874600\
0412516173477464286587885568673774760377090940027
```

We know how to avoid computing huge intermediate numbers. Sage does the same if we instead use something like:

```
Sage] power_mod(3, 1003, 101)
```

```
27
```

10 Gossip

Newsflash. Yesterday, Sir Michael Atiyah, who won the Fields medal in 1966, claimed (at the (prime!) age of 89) a proof of the Riemann hypothesis. Unfortunately, his lecture (as well a draft circulated online) are overly casual and do not contain what is recognizable as a full proof.

https://www.heidelberg-laureate-forum.org/blog/video/lecture-monday-september-24-2018-sir-michael-francis-atiyah/

Example 76. (Riemann hypothesis) The **Riemann zeta function** $\zeta(s)=\sum_{n\geqslant 1}\frac{1}{n^s}$ converges (for real s) if and only if $s>1$.

The divergent series $\zeta(1)$ is the harmonic series, and $\zeta(p)$ is often called a p-series in Calculus II.

Comment. Euler achieved worldwide fame by discovering and proving that $\zeta(2)=\frac{\pi^2}{6}$ (and similar formulas for $\zeta(4),\zeta(6),\ldots$).

For complex values of $s\neq 1$, there is a unique way to "analytically continue" this function. It is then "easy" to see that $\zeta(-2)=0$, $\zeta(-4)=0$, ... The **Riemann hypothesis** claims that all other zeroes of $\zeta(s)$ lie on the line $s=\frac{1}{2}+a\sqrt{-1}$ ($a\in\mathbb{R}$). A proof of this conjecture (checked for the first 10,000,000,000,000 zeroes) is worth $1,000,000.

http://www.claymath.org/millennium-problems/riemann-hypothesis

The connection to primes. Here's a vague indication that $\zeta(s)$ is intimately connected to prime numbers:

$$\begin{aligned}\zeta(s) &= \left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\ldots\right)\left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\ldots\right)\left(1+\frac{1}{5^s}+\frac{1}{5^{2s}}+\ldots\right)\cdots\\ &= \frac{1}{1-2^{-s}}\frac{1}{1-3^{-s}}\frac{1}{1-5^{-s}}\cdots\\ &= \prod_{p\text{ prime}}\frac{1}{1-p^{-s}}\end{aligned}$$

This infinite product is called the Euler product for the zeta function. If the Riemann hypothesis was true, then we would be better able to estimate the number $\pi(x)$ of primes $p\leqslant x$.

More generally, certain statements about the zeta function can be translated to statements about primes. For instance, the (non-obvious!) fact that $\zeta(s)$ has no zeros for $\operatorname{Re}s=1$ implies the prime number theorem that we discussed last time.

http://www-users.math.umn.edu/~garrett/m/v/pnt.pdf