

Re: Mod 2011

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-01/msg03212.html>

- *From:* Gerry Myerson <gerry@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 17 Jan 2007 00:06:22 GMT
-

In article <87ps9esi4k.fsf@xxxxxxxxxxxxxxxxxxxxxxxx>, Phil Carmody <thefatphil_demunged@xxxxxxxxxxxx> wrote:

erick@xxxxxx (Erick Bryce Wong) writes:

Jyrki Lahtonen <lahtonen@xxxxxx> wrote:

"Jyrki Lahtonen" <lahtonen@xxxxxx>
wrote in message
[news:eoibr0\\$1ac0\\$2@xxxxxxxxxxxxxxxxxxxx](mailto:news:eoibr0$1ac0$2@xxxxxxxxxxxxxxxxxxxx)

León-Sotelo wrote:

Determine
the
remainder
when $1004!$
is divided
by 2011.

In that case Wilson's theorem says that $2010!$ is congruent to minus 1 modulo 2011. The rest is easy.

How does one easily resolve the issue of whether $1005!$ is +1 or -1?

Here's some jibber-jabber I threw together 6 months ago on a mailing list:

<http://tech.groups.yahoo.com/group/primenumbers/message/18206?threaded=1&var=1&l=1>

<<<
Factorial flight of fancy

=====
I'm not expecting this to lead anywhere, but I don't think I've seen these ideas approached from this particular angle before. I suspect almost everything is trivial and well-known.

It's long and rambling – print it out and take it with you to the thinking room next time you go there!

I'm looking at vanishing values of $n! \pmod{q} \pm 1$ for q prime, $n < q$.

(Can you tell I've been sieving for factorial primes?)

So let's fix q , and work in the ring of integers modulo q . The process of evaluating $n!$ for each n is a simple iterative process, highly regular, and with clearly defined starting points and ending points.

The sequence always starts:
 $1! \pmod{q} = +1$

And it always ends:
 $(q-2)! \pmod{q} = +1$
 $(q-1)! \pmod{q} = -1$
(c.f. Wilson's theorem)

I find the 'gentle landing' most appealing, I synaesthetically picture the residues as behaving like a quantum packet starting at, and fading to, nothing, but having wild perturbations in the middle:

```
vV VVVVVv
--^|||||||_--
^^W W W W^^
```

Very unlike traditional stochastic behaviour due to the gentle landing at the end. So perhaps the behaviour of the residues within the superficially chaotic area in the middle will have some interesting patterns.

The first thing to notice is that the pattern of the residues has a symmetry to it.

$$i! * (q-1-i)! \pmod{q} = \pm 1$$

Therefore if $i! \pmod{q} \pm 1$ vanishes modulo q , then so does $(q-1-i)! \pmod{q} \pm 1$.

If one is like me, one is then immediately led to wonder if there are primes q for which the exact middle point, $((q-1)/2)! \pmod{q} \pm 1$, vanishes. In fact, they aren't rare at all:

```
pptest(p)={
local(pr=1);
```

```

print1("P = "p" :");
for(i=2,(p-1)/2,
pr=pr*i%p;
if(pr==1,print1(" "i!"-1%p));
if(pr==p-1,print1(" "i!"+1%p))
);
print(if(pr^2%p==1,"=middle",""))
)
forprime(pt=5,100,ptest(pt))

```

```

P = 5 :
P = 7 : 3!+1%7=middle
P = 11 : 5!+1%11=middle
P = 13 :
P = 17 : 5!-1%17
P = 19 : 9!+1%19=middle
P = 23 : 4!-1%23 8!-1%23 11!-1%23=middle
P = 29 : 10!-1%29
P = 31 : 15!-1%31=middle
P = 37 :
P = 41 :
P = 43 : 21!+1%43=middle
P = 47 : 23!+1%47=middle
P = 53 : 15!-1%53
P = 59 : 15!+1%59 18!-1%59 29!-1%59=middle
P = 61 : 8!+1%61 16!+1%61 18!+1%61
P = 67 : 18!+1%67 33!+1%67=middle
P = 71 : 7!+1%71 9!+1%71 19!+1%71 35!-1%71=middle
P = 73 : 17!-1%73
P = 79 : 23!+1%79 39!+1%79=middle
P = 83 : 13!+1%83 36!+1%83 41!-1%83=middle
P = 89 : 21!-1%89
P = 97 : 43!-1%97

```

Summarising:

- a) Primes with +1 at the middle: 3,23,31,59,71,83,...
- b) Primes with -1 at the middle: 7,11,19,43,47,67,79,...
- c) Primes without +/-1 at the middle: 5,13,17,29,37,41,53,61,73,89,97,...

The pattern behind the dichotomy "+/-1 or not" should have been detected after only a few terms. Obviously the families $q=4n+1$ and $q=4n+3$ have different behaviour.

That might ring 'jacobi(-1,q)' bells, and one is compelled to investigate whether square roots of -1 are in any way relevant.

Changing the above GP script's final print statement to `if(pr^2%p==1,print("=middle"),print(" "pr":"(pr^2+1)%p-1"))` the investigation leads to an instant conclusion:

```
P = 5 : (2:-1)
```

$P = 13 : (5:-1)$
 $P = 17 : 5!-1\%17 (13:-1)$
 $P = 29 : 10!-1\%29 (12:-1)$
 $P = 37 : (31:-1)$
 $P = 41 : (9:-1)$
 $P = 53 : 15!-1\%53 (23:-1)$
 $P = 61 : 8!+1\%61 16!+1\%61 18!+1\%61 (11:-1)$
 $P = 73 : 17!-1\%73 (27:-1)$
 $P = 89 : 21!-1\%89 (34:-1)$
 $P = 97 : 43!-1\%97 (22:-1)$

Quite simply – if a square root of -1 modulo q exists, it is $((q-1)/2)!$

So apparently we've completely tamed the very centre of that quantum packet above. It's either $+/-1$, or $\text{sqrt}(-1)$, depending on $q\%4$.

Curiously, this gives us a deterministic way of uniquely specifying a 4th root of unity modulo q . That's something we can't do in \mathbb{C} , as $+/-i$ are indistinguishable due to the field automorphism that exists.

Of course, these numerical curiosities are nothing more than observation as presented. I don't believe proofs that they are not just a coincidence should be too hard. In textbook style, I should leave them as an exercise for the reader (and of course the writer).

And once that's been done, the open questions remain –

1) What's the difference between primes in sequences (a) and (b) above?

They are already on OEIS, but with no explanation:

<http://www.research.att.com/~njas/sequences/A058302>

<http://www.research.att.com/~njas/sequences/A055939>

2) Are there other points apart from the very middle and the ends where the sequence can be so simply tamed?

3) Do higher roots of unity occur with any regularity?

E.g. for sequence (c), where the primes q do have $\text{sqrt}(-1)$, does the sequence $p!\%q+/-\text{sqrtmod}(-1,q)$ vanish at any predictable points?

$P = 37 : 3!+/-i\%37$
 $P = 61 : 21!+/-i\%61$
 $P = 89 : 40!+/-i\%89$
 $P = 101 : 7!+/-i\%101 12!+/-i\%101$
 $P = 109 : 14!+/-i\%109$
 $P = 113 : 27!+/-i\%113$
 $P = 149 : 16!+/-i\%149$
 $P = 157 : 21!+/-i\%157$
 $P = 173 : 51!+/-i\%173$
 $P = 181 : 58!+/-i\%181$
 $P = 193 : 34!+/-i\%193 69!+/-i\%193 79!+/-i\%193$

Re: Mod 2011

$P = 197 : 82! \pm i \% 197$

I don't see a pattern.

4) Do double factorials (or higher) have similar properties?
(I suspect that the double might have, but I've not checked any values at all.)

Does anyone else have any insights into these matters?

It's shown in Niven, Zuckerman, and Montgomery that if p is $1 \pmod{4}$ then $((p-1)/2)!$ squared is $-1 \pmod{p}$ (p. 54), and it's an exercise to show that if p is $3 \pmod{4}$ then the quantity is plus-or-minus 1 (exercise 2.1.18).

Maybe something interesting happens with $((p-1)/3)!$ factorial, for those primes congruent $1 \pmod{3}$.

--

Gerry Myerson (gerry@xxxxxxxxxxxxxxxx) (i -> u for email)

.