University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Homework questions – Week 6

Jean-Baptiste Campesato

March 1st, 2021 to March 5th, 2021

Hint: all these exercises can be solved using Fermat's little theorem and/or Wilson's theorem.

Exercise 1.
Find the remainder of the Euclidean division of 24^{103} by 103.

Exercise 2.

Prove that $\forall n \in \mathbb{Z},\ \frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$.

You may already use $\mathbb{Q}$ for this question.
Hint: *introduce* $A_n = 35\left(\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35}\right)$.

Exercise 3.
Let p be an odd prime number. Prove that $\forall n \in \mathbb{Z},\ (n+1)^p - (n^p + 1) \equiv 0 \pmod{2p}$.

Exercise 4.

Let p be a prime number. Prove that $\forall k \in \mathbb{N},\ \forall n \in \mathbb{Z} \setminus \{0\},\ \gcd(n,p) = 1 \implies \left(n^{p-1}\right)^{p^k} \equiv 1 \pmod{p^{k+1}}$.

Exercise 5.
Let p and q be two distinct prime numbers. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Exercise 6.
Prove that $x^4 + 781 = 3y^4$ has no integer solution.

Exercise 7.
Let $n \in \mathbb{N}$ be such that $n \geq 5$. Prove that if $n+2$ is prime then $n! - 1$ is composite.

Exercise 8.
Let p be an odd prime number. Prove that $2(p-3)! \equiv -1 \pmod{p}$.

Exercise 9. *A characterization of twin prime numbers.*
Let $n \in \mathbb{N} \setminus \{0,1\}$. Prove that if n and $n+2$ are both prime numbers then

$$4\left((n-1)! + 1\right) + n \equiv 0 \pmod{n(n+2)}$$

(*Actually the converse holds too, but it's a little bit more difficult to prove*)

Exercise 10.
Let p be a prime number. Prove that $\forall n \in \mathbb{Z},\ p | n^p + (p-1)!n$.

Sample solutions to Exercise 1.
By Fermat's little theorem, we know that $24^{103} \equiv 24 \pmod{103}$.
Therefore the remainder of the Euclidean division of 24^{103} by 103 is 24.

Sample solutions to Exercise 2.
Let $n \in \mathbb{Z}$. Set $A_n = 5n^7 + 7n^5 + 23n$.
By Fermat's little theorem, $n^5 \equiv n \pmod 5$ so $A_n \equiv 30n \pmod 5 \equiv 0 \pmod 5$, i.e. $5|A_n$.
Similarly $n^7 \equiv n \pmod 7$, so $A_n \equiv 28n \pmod 7 \equiv 0 \pmod 7$, i.e. $7|A_n$.
Therefore $35 = 5 \times 7 | A_n$, so $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} = \frac{A_n}{35} \in \mathbb{Z}$.

Sample solutions to Exercise 3.
Let p be an odd prime number and $n \in \mathbb{Z}$.

- By Fermat's little theorem, $\begin{cases} (n+1)^p \equiv n+1 \pmod p \\ n^p \equiv n \pmod p \end{cases}$
  Therefore $(n+1)^p - (n^p+1) \equiv 0 \pmod p$, i.e. $p|(n+1)^p - (n^p+1)$.
- Note that $\forall x \in \mathbb{Z}$, $\forall k \in \mathbb{N} \setminus \{0\}$, $x^k \equiv x \pmod 2$:

$a \pmod 2$	0	1
$a^2 \pmod 2$	0	1

  Therefore $\begin{cases} (n+1)^p \equiv n+1 \pmod 2 \\ n^p \equiv n \pmod 2 \end{cases}$.
  Thus $(n+1)^p - (n^p+1) \equiv 0 \pmod 2$, i.e. $2|(n+1)^p - (n^p+1)$.

Since 2 and p are two distinct prime numbers, $2p|(n+1)^p - (n^p+1)$, i.e. $(n+1)^p - (n^p+1) \equiv 0 \pmod{2p}$.

Sample solutions to Exercise 4.
We are going to prove the statement by induction on $k \in \mathbb{N}$.

- *Base case at $k = 0$:* it is exactly Fermat's little theorem (v2).
- *Induction step:* assume that the statement hold for some $k \in \mathbb{N}$, i.e.

$$\forall n \in \mathbb{Z} \setminus \{0\},\ \gcd(n,p) = 1 \implies \left(n^{p-1}\right)^{p^k} \equiv 1 \pmod{p^{k+1}}$$

  Let $n \in \mathbb{Z}$ be such that $\gcd(n,p) = 1$.
  By induction hypothesis, there exists $\lambda \in \mathbb{Z}$ such that $\left(n^{p-1}\right)^{p^k} = 1 + \lambda p^{k+1}$. Then

$$\left(n^{p-1}\right)^{p^{k+1}} = \left(n^{p-1}\right)^{p^k \times p} = \left(\left(n^{p-1}\right)^{p^k}\right)^p = \left(1+\lambda p^{k+1}\right)^p = \sum_{i=0}^{p} \binom{p}{i} \lambda^i p^{i(k+1)} = 1 + \sum_{i=1}^{p} \binom{p}{i} \lambda^i p^{i(k+1)} \equiv 1 \pmod{p^{k+1}}$$

  Which ends the induction step.

Sample solutions to Exercise 5.
Let p and q be two distinct prime numbers.
Since $\gcd(p,q) = 1$, by Fermat's little theorem we get that $p^{q-1} \equiv 1 \pmod q$.
Besides $q^{p-1} \equiv 0 \pmod q$ (since $p \geq 2$).
Therefore $p^{q-1} + q^{p-1} \equiv 1 \pmod p$, i.e. $p|\left(p^{q-1} + q^{p-1} - 1\right)$.
Similarly, we may prove that $q|\left(p^{q-1} + q^{p-1} - 1\right)$.
Thus $pq|\left(p^{q-1} + q^{p-1} - 1\right)$.

Sample solutions to Exercise 6.
Let $x, y \in \mathbb{Z}$.
By Fermat's little theorem, $x^4 \equiv 1 \pmod 5$ (if $5 \nmid x$) or $x^4 \equiv 0 \pmod 5$ (if $5|x$).
Therefore $x^4 + 781 \equiv 1 \pmod 5$ or $x^4 + 781 \equiv 2 \pmod 5$.
But $3y^4 \equiv 3 \pmod 5$ (if $5 \nmid y$) or $3y^4 \equiv 0 \pmod 5$ (if $5|y$).
Therefore $\forall x, y \in \mathbb{Z},\ x^4 + 781 \not\equiv 3y^4 \pmod 5$.

Sample solutions to Exercise 7.
Let $n \geq 5$ be such that $n + 2$ is prime.
By Wilson's theorem $(n + 1)! \equiv -1 \pmod{n + 2}$. Thus $n + 2|(n + 1)! + 1$.
Besides $(n + 1)! + 1 = (n + 2)n! - n! + 1$.
Thus $n + 2|n! - 1 = (n + 2)n! - ((n + 1)! + 1)$.
Since $n \geq 4$, we have $n! > n + 3$ (*prove it*).
Therefore $n! - 1$ admits at least three positive divisors: $1, n + 2, n! - 1$, so that n is composite.

Sample solutions to Exercise 8.
Let p be an odd prime number.
By Wilson's theorem $(p - 1)! \equiv -1 \pmod p$, thus $2(p - 3)!(p - 2)(p - 1) \equiv -2 \pmod p$.
But we also have that $2(p - 3)!(p - 2)(p - 1) \equiv 4(p - 3)! \pmod p$.
Thus $4(p - 3)! \equiv -2 \pmod p$, i.e. $p|4(p - 3)! + 2 = 2(2(p - 3)! + 1)$.
Since $\gcd(2, p) = 1$ (as p is an odd prime number), by Gauss' lemma we get $p|2(p - 3)! + 1$,
i.e. $2(p - 3)! \equiv -1 \pmod p$.

Sample solutions to Exercise 9.
$\Rightarrow$ Assume that n and $n + 2$ are both prime then,

- By Wilson's theorem, $(n - 1)! \equiv -1 \pmod n$, so $4((n - 1)! + 1) + n \equiv 0 \pmod n$,
  i.e. $n|4((n - 1)! + 1) + n$.
- By Wilson's theorem, $(n + 1)! \equiv -1 \pmod{n + 2}$.
  Besides $2 \equiv -n \pmod{n + 2} \equiv (n + 1)n \pmod{n + 2}$.
  Thus
  $4((n-1)!+1)+n = 2(2(n-1)!)+4+n \equiv 2((n+1)n(n-1)!)+2 \pmod{n+2} \equiv 2((n+1)!+1) \equiv 0 \pmod{n+2}$
  i.e. $n + 2|4((n - 1)! + 1) + n$.

Since $\gcd(n, n + 2) = 1$, we get that $n(n + 2)|4((n - 1)! + 1) + n$.

Sample solutions to Exercise 10.
Let p be a prime number. Let $n \in \mathbb{Z}$.
By Fermat's little theorem $n^p \equiv n \pmod p$ and by Wilson's theorem $(p - 1)! \equiv -1 \pmod p$.
Therefore $n^p + (p - 1)!n \equiv n + (-1)n \pmod p \equiv 0 \pmod p$.