1

13/20

MAT246 HW2 Rui Qiu #999292509

(1) Give a proof by induction of the following theorem from class.
Let $m>1$ be a natural number. Then for any $n\geq 0$ there exists an integer $r$ such that $0\leq r<m$ and $n\equiv r \pmod m$

Proof:

For $n=0$, let $r=n=0$, then $0\leq 0<m$ and $0\equiv 0 \pmod m$)
Suppose the claim holds for $n$. $\exists r\in\mathbb{Z}$ st. $0\leq r<m$ and $n\equiv r \pmod m$.
i.e. $n=mq+r$, $q\in\mathbb{N}$
so $n+1=mq+r+1=mq+r'$
this also holds for $n+1$.
Therefore the claim holds for all $n\geq 0$.

You need to make sure $r+1<m$

(2). Let $p_1, p_2$ be distinct primes. Using the Fundamental Theorem of Arithmetic prove that a natural number $n$ is divisible by $p_1p_2$ if and only if $n$ is divisible by $p_1$ and $n$ is divisible by $p_2$.

Proof: $\Rightarrow$ If $n$ is divisible by $p_1$ and $n$ is divisible by $p_2$ ($n>1$ since the smallest prime is $2>1$)
then by Fundamental Theorem of Arithmetic that every natural number greater than 1 can be written as a product of primes that
$n=p_1p_2\cdots p_k$, $p_i$ is prime, $i\in\mathbb{N}^+$.
so $n$ is also divisible by $p_1p_2$.

where do you use distinct?

$\Leftarrow$ If $n$ is divisible by $p_1p_2$
similarly by Fundamental Theorem of Arithmetic that
$n=p_1p_2p_3\cdots p_k$. $p_i$ is prime, $i\in\mathbb{N}^+$.
therefore, $n$ is divisible by $p_1$ and $p_2$.

(3). Prime 'triplets' are triples of prime numbers of the form $n, n+2, n+4$.
Find all prime triples.
Hint: Think (mod 3)

Solution.

Since $n+4 \equiv n+1 \pmod 3$
then for $n, n+2, n+4$, one of them must be divisible by 3.
So the number would be a composite unless it is prime, i.e. it is 3.
when $n=3$, $n+2=5$, $n+4=7$, it is a prime triple.
when $n+2=3$, $n=1$, not a prime
when $n+4=3$, $n=-1$, not a prime
Therefore 3, 5, 7 is the only prime triple.

(4). (a) Find all possible values of $2^k \pmod 6$
(b). Find all possible values of $k^2 \pmod 6$

Solution: (a).
$$2^0 = 1 \equiv 1 \pmod 6$$
$$2^1 = 2 \equiv 2 \pmod 6$$
$$2^2 = 4 \equiv 4 \pmod 6$$
$$2^3 = 8 \equiv 2 \pmod 6$$
$$2^4 = 16 \equiv 4 \pmod 6$$
$$\cdots$$
$$2^{2k-1} \equiv 2 \pmod 6$$
$$2^{2k} \equiv 4 \pmod 6 \quad \text{for } k \in \mathbb{N}^+$$
$$2^0 \equiv 1 \pmod 6$$

Therefore the possible values of $2^k \pmod 6$ are 1, 2, 4.

(b).
$$0^2 = 0 \equiv 6 \pmod 6$$
$$1^2 = 1 \equiv 1 \pmod 6$$
$$2^2 = 4 \equiv 4 \pmod 6$$
$$3^2 = 9 \equiv 3 \pmod 6$$
$$4^2 = 16 \equiv 4 \pmod 6$$
$$5^2 = 25 \equiv 1 \pmod 6$$
$$6^2 = 36 \equiv 6 \pmod 6$$
$$7^2 = 49 \equiv 1 \pmod 6$$
$$8^2 = 64 \equiv 4 \pmod 6$$
$$9^2 = 81 \equiv 3 \pmod 6$$
$$10^2 = 100 \equiv 4 \pmod 6$$
$$11^2 = 121 \equiv 1 \pmod 6$$

MAT246 HW2 Rui Qiu #999292509

$(6k)^2 \equiv 6 \pmod 6$

$(6k+1)^2 \equiv 1 \pmod 6$

$(6k+2)^2 \equiv 4 \pmod 6$

$(6k+3)^2 \equiv 3 \pmod 6$

$(6k+4)^2 \equiv 4 \pmod 6$

$(6k+5)^2 \equiv 1 \pmod 6$

Therefore the possible values of $k^2 \pmod 6$ are 1, 3, 4 and 6.

(5). Prove that for any natural $k$.

$$4^k + 4\cdot 9^k \equiv 0 \pmod 5$$

Proof: For $4^k$ we have $\begin{cases} 4^{2m} \equiv 1 \pmod 5 \\ 4^{2m+1} \equiv 4 \pmod 5 \end{cases}$ for $m \in \mathbb{N}$.

For $4\cdot 9^k$ we have $\begin{cases} 4\cdot 9^{2n} \equiv 4 \pmod 5 \\ 4\cdot 9^{2n+1} \equiv 1 \pmod 5 \end{cases}$ for $n \in \mathbb{N}$.

Let $m=n=r$, by theorem 3.1.5 that

$$\begin{cases} 4^{2r} + 4\cdot 9^{2r} \equiv 1+4 \equiv 0 \pmod 5 \\ 4^{2r+1} + 4\cdot 9^{2r+1} \equiv 4+1 \equiv 0 \pmod 5 \end{cases}$$

Hence for all natural $k$, $4^k + 4\cdot 9^k \equiv 0 \pmod 5$ ∎

(6). Find the rule for checking when an integer is divisible by 13 similar to the rule for checking divisibility by 7 done in class.

Solution:

First we know that for a number $n = \overline{a_k a_{k-1} \cdots a_2 a_1 a_0}$, $k \in \mathbb{N}$ and every $a_i$ is a two-digit number, $i \in \mathbb{N}$.

So $n = a_0 + a_1 \cdot 10^2 + a_2 \cdot 10^4 + \cdots + a_k \cdot 10^{2k}$

$10^0 \equiv 1 \pmod{13}$

$10^2 \equiv 9 \pmod{13}$

$10^4 \equiv 3 \pmod{13}$

$10^6 \equiv 1 \pmod{13}$

$10^8 \equiv 9 \pmod{13}$

$10^{10} \equiv 3 \pmod{13}$

...

So $10^{6k} \equiv 1 \pmod{13}$

$10^{6k+2} \equiv 9 \pmod{13}$

$10^{6k+4} \equiv 3 \pmod{13}$

Therefore $n = a_0 + a_1 \cdot 10^2 + a_2 \cdot 10^4 + \cdots + a_k \cdot 10^{2k}$

$\equiv 1 \cdot a_0 + 9 \cdot a_1 + 3a_2 + 1 \cdot a_3 + 9 \cdot a_4 + 3a_5 + \cdots \pmod{13}$

$\equiv 1 \cdot (a_{3n}) + 9(a_{3n+1}) + 3(a_{3n+2}) \pmod{13}$

(7) Prove that if $m > 1$ is not prime then there exist integers $a, b, c$ such that $c \not\equiv 0 \pmod m$, $ac \equiv bc \pmod m$ but $a \not\equiv b \pmod m$

Proof: Since $m$ is not prime, then it must be a composite

Say $m = xy$ for $x \neq 1, y \neq 1$, $x, y \in \mathbb{N}^+$.

So we now have:

$c \not\equiv 0 \pmod{xy}$

$ac \equiv bc \pmod{xy}$

$a \not\equiv b \pmod{xy}$

And $xy \equiv 0 \bmod xy$

Let $c = x$, then $c \not\equiv 0 \pmod{xy}$, since $0 < c < xy$.

then let $a = y$, $b = 0$

Now we have $ac \equiv xy \equiv 0 \cdot y \equiv b \cdot c \pmod{xy}$

Finally $y \not\equiv 0 \pmod{xy}$ since $0 < y < xy$.

The claim is proved.

MAT246 HW2 Rui Qiu #999292509

Problems on textbook

Page 30.

#3 (a, b, d)

(a) $3^{2463}$ is divided by 8.

Solution: $3^0 \equiv 1 \pmod 8$

$3^1 \equiv 3 \pmod 8$

$3^2 \equiv 1 \pmod 8$

$3^3 \equiv 3 \pmod 8$

...

$3^{2n} \equiv 1 \pmod 8$

$3^{2n+1} \equiv 3 \pmod 8$, $n \in \mathbb{N}$

So $3^{2463} \equiv 3^{1231 \times 2 + 1} \equiv 3 \pmod 8$

i.e. the remainder is 3.

(b). $2^{923}$ is divided by 15.

Solution: $2^0 \equiv 1 \pmod{15}$

$2^1 \equiv 2 \pmod{15}$

$2^2 \equiv 4 \pmod{15}$

$2^3 \equiv 8 \pmod{15}$

$2^4 \equiv 1 \pmod{15}$

$2^5 \equiv 2 \pmod{15}$

$2^6 \equiv 4 \pmod{15}$

$2^7 \equiv 8 \pmod{15}$

...

$2^{4n} \equiv 1 \pmod{15}$

$2^{4n+1} \equiv 2 \pmod{15}$

$2^{4n+2} \equiv 4 \pmod{15}$

$2^{4n+3} \equiv 8 \pmod{15}$, $n \in \mathbb{N}$

So $2^{923} \equiv 2^{230 \times 4 + 3} \equiv 8 \pmod{15}$

i.e. the remainder is 8.

10. $5^{2001}+(27)!$ is divided by 8.

Solution: $5^0 \equiv 1 \pmod 8$

$5^1 \equiv 5 \pmod 8$

$5^2 \equiv 1 \pmod 8$

$5^3 \equiv 5 \pmod 8$

....

$5^{2n} \equiv 1 \pmod 8$

$5^{2n+1} \equiv 5 \pmod 8$ $\quad n \in \mathbb{N}$ $\quad$ so $5^{2001} \equiv 5^{2\times1000+1} \equiv 5 \pmod 8$.

Since $(27)! = 1\times2\times3\times4\times5\times6\times7\times8\times\cdots\times27$

So $(27)! \equiv 0 \pmod 8$

By Theorem 3.1.5 that

$5^{2001}+(27)! \equiv 5+0 \equiv 5 \pmod 8$

i.e. the remainder is 5.

#12. Prove that 21 divides $3n^7+7n^3+11n$ for every number $n$.

Proof We want to prove $3n^7+7n^3+11n$ is divisive by 3 and 7.

For mod 3.

For $3n^7 \equiv 0 \pmod 3$

If $n \equiv 0 \pmod 3$

then $7n^3 \equiv 0 \pmod 3$

$11n \equiv 0 \pmod 3$

so $3n^7+7n^3+11n \equiv 0 \pmod 3$

If $n \equiv 1 \pmod 3$

then $7n^3 \equiv 1 \pmod 3$

$11n \equiv 2 \pmod 3$

So $3n^7+7n^3+11n \equiv 0+1+2 \equiv 0 \pmod 3$

If $n \equiv 2 \pmod 3$

then $7n^3 \equiv 7\cdot2^3 \equiv 2 \pmod 3$

$11n \equiv 22 \equiv 1 \pmod 3$

So $3n^7+7n^3+11n \equiv 0+2+1 \equiv 0 \pmod 3$

Hence $3n^7+7n^3+11n$ is divisive by 3

Then for mod 7

Basically we use the same idea to test

MAT246 HW2 Rui Qiu #999292509

If $n \equiv 0 \pmod 7$, $3n^7 + 7n^3 + 11n \equiv 0 \pmod 7$

$n \equiv 1 \pmod 7$,

then $3n^7 \equiv 3(1)^7 \equiv 3 \pmod 7$

$11n \equiv 4 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 3 + 0 + 4 \equiv 0 \pmod 7$

$n \equiv 2 \pmod 7$

then $3n^7 \equiv 3(2)^7 \equiv 6 \pmod 7$

$11n \equiv 22 \equiv 1 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 6 + 0 + 1 \equiv 0 \pmod 7$

$n \equiv 3 \pmod 7$

then $3n^7 \equiv 3 \times 3^7 \equiv 2 \pmod 7$

$11n \equiv 33 \equiv 5 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 2 + 0 + 5 \equiv 0 \pmod 7$

$n \equiv 4 \pmod 7$

then $3n^7 \equiv 3 \times 4^7 \equiv 5 \pmod 7$

$11n \equiv 44 \equiv 2 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 5 + 0 + 2 \equiv 0 \pmod 7$

$n \equiv 5 \pmod 7$

then $3n^7 \equiv 3 \times 5^7 \equiv 1 \pmod 7$

$11n \equiv 55 \equiv 6 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 1 + 0 + 6 \equiv 0 \pmod 7$

$n \equiv 6 \pmod 7$

then $3n^7 \equiv 3 \times 6^7 \equiv 4 \pmod 7$

$11n \equiv 66 \equiv 3 \pmod 7$

So $3n^7 + 7n^3 + 11n \equiv 4 + 0 + 3 \equiv 0 \pmod 7$

Therefore $3n^7 + 7n^3 + 11n$ is divisible by 7.

So $3n^7 + 7n^3 + 11n$ is divisible by 21. ∎

#19. Prove that 133 divides $11^{n+1}+12^{2n-1}$ for every natural number $n$.

Proof. This problem is quite similar as last problem, we want to prove $11^{n+1}+12^{2n-1}$ is divisible by $133 = 9\times 17$, so what we need to do is just to prove $11^{n+1}+12^{2n-1}$ is divisible by 9 and 17 separately.

(See page 5)

✓ #26. Prove that there are an infinite number of primes of the form $4k+3$ with $k$ a natural number. [Hint: If $p_1, \cdots, p_n$ are $n$ such primes, show that $4(p_1p_2p_3\cdots p_n)-1$ ~~is~~ has at least one prime divisor of the ~~the~~ given form.

Proof: Suppose there are only finitely many primes $p_1=3, \cdots, p_n$. Then we consider a number $4(p_1p_2p_3\cdots p_n)-1$, it is in form of $4n+3$, but larger than $p_n$, so it is not a prime.

Therefore it is divisible by a prime.

Since $p_i \nmid 4(p_1p_2p_3\cdots p_n)-1$,

so all primes that divide $4(p_1p_2p_3\cdots p_n)-1$ are of form $4n+1$

But for $(4n+1)(4m+1) = 16mn+4m+4n+1 = 4(4mn+m+n)+1$

Therefore the products of form $4n+1$ primes are always in $4n+1$, which contradicts the assumption

(the assumption is a $4n-1$ form).

Hence there are infinitely many primes of the form $4k+3$.

■

5

MAT246 HW2 Rui Qiu #999292509

#19.

Proof: We want to prove 133 divides $11^{n+1}+12^{2n-1}$, and this can be proved by the divisibilities of 7 and 19.

Check mod 7.

$$
\begin{aligned}
& 11^{n+1}+12^{2n-1} \\
\equiv\ & 4^{n+1}+5^{2n-1} \pmod 7 \\
\equiv\ & 4^{n+1}+(25)^{n}\cdot\tfrac{1}{5} \pmod 7 \\
\equiv\ & 4^{n+1}+4^{n}\cdot 3 \pmod 7 \\
\equiv\ & (4+3)\,4^{n} \pmod 7 \\
\equiv\ & 7\cdot 4^{n} \pmod 7 \\
\equiv\ & 0 \pmod 7
\end{aligned}
$$

So 7 divides $11^{n+1}+12^{2n-1}$.

Check mod 19

$$
\begin{aligned}
& 11^{n+1}+12^{2n-1} \\
\equiv\ & 11^{n+1}+(12^{2})^{n}\,12^{-1} \pmod{19} \\
\equiv\ & 11^{n+1}+11^{n}\,8 \pmod{19} \\
\equiv\ & 11^{n}(11+8) \pmod{19} \\
\equiv\ & 19\cdot 11^{n} \pmod{19} \\
\equiv\ & 0 \pmod{19}
\end{aligned}
$$

So 19 also divides $11^{n+1}+12^{2n-1}$.

Therefore 133 divides $11^{n+1}+12^{2n-1}$ for all natural $n$. ∎