MAT246: Concepts in Abstract Mathematics:
Lecture 0101 Notes

Tianyu Du

September 26, 2018

Contents

1 Lecture 1 Sep. 7 2018 **2**

2 Lecture 2 Sep. 10 2018 **2**

3 Lecture 3 Sep. 12 2018 **3**

4 Lecture 4 Sep. 14 2018 **4**

5 Lecture 5 Sep. 17 2018 **5**

6 Lecture 6 Sep. 19 2018 **7**

7 Lecture 7 Sep. 21 2018 **8**

8 Lecture 8 Sep. 24 2018 **9**

9 Lecture 9 Sep. 26 2018 **11**

1 Lecture 1 Sep. 7 2018

Definition 1.1. Let $\mathbb{N} := \{1, 2, 3, \dots\}$ be the set of **natural numbers**.

Theorem 1.1 (Principle of Mathematical Induction)**.** Suppose S is a set of natural numbers, $S \subseteq \mathbb{N}$. If

1. $1 \in S$
2. $k \in S \implies k + 1 \in S,\ \forall k \in \mathbb{N}$

then, $S = \mathbb{N}$

Example 1.1. Show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}\ \forall n \in \mathbb{N}$$

Proof. ■

2 Lecture 2 Sep. 10 2018

Theorem 2.1 (Extended Principle of Mathematical Induction)**.** Suppose set $S \subseteq \mathbb{N}$ and let $n_0 \in \mathbb{N}$ fixed, if

1. $n_0 \in S$
2. $\forall k \geq n_0, k \in S \implies k + 1 \in S$

then $\{n_0, n_0 + 1, n_0 + 2, \dots\} \subseteq S$

Example 2.1. Show that

$$n! \geq 3^n\ \forall n \geq 7$$

Proof. ■

Theorem 2.2 (Well-Ordering Principle)**.** Every non-empty subset of natural number has a smallest element.

Proof. (Principle of Mathematical Induction)
Let $S \subseteq \mathbb{N}$
Suppose $1 \in S \wedge (k \in S \implies k + 1 \in S, \forall k \in \mathbb{N})$
Show: $S = \mathbb{N}$
Let $T = \mathbb{N} \backslash S$

Suppose $T \neq \emptyset$
By Well-Ordering Principle, there exists a smallest element of T, denoted as $t_0 \in \mathbb{N}$.
Since $1 \in S$, therefore $t_0 \neq 1$.
Therefore $t_0 > 2$.
Thus $t_0 - 1 \in \mathbb{N}$ and since $t_0 = \min T$, $t_0 - 1 \notin T$
Therefore $t_0 - 1 \in S$, then, $t_0 - 1 + 1 = t_0 \in S$,
Contradict the assumption that $t_0 \in T$.
Thus $T = \emptyset$ and $S = \mathbb{N}$.

■

Remark 2.1. We can use principle of Mathematical Induction to prove Well-Ordering Principle as well.

3 Lecture 3 Sep. 12 2018

Definition 3.1. Let $a, b \in \mathbb{N}$ and a **divides** b, written as $a|b$ if

$$\exists c \in \mathbb{N} \ s.t. \ b = ac$$

And a is a **divisor** of b.

Definition 3.2. A natural number p (except 1) is called **prime** if the only divisors of p are 1 and p.

Lemma 3.1 (Prime numbers are building blocks of natural numbers)**.** Every natural number other than 1 is a *product*[1] of prime numbers.

Theorem 3.1 (Principle of Complete Induction)**.** Suppose $S \subseteq \mathbb{N}$ and if

1. $n_0 \in S$
2. $n_0, n_0 + 1, \ldots, k \in S \implies k + 1 \in S, \ \forall k \geq n_0$

then

$$\{n_0, n_0 + 1, \ldots\} \subseteq S$$

Proof of Lemma. Let $S \subseteq \mathbb{N}$ for which the lemma is true,
Want to show: $S = \mathbb{N} \backslash \{1\}$
(Base Case) For 2 it's a product of prime. Thus $2 \in S$
(Inductive Step) Suppose $\{2, 3, \ldots k\} \subseteq S$

[1]Product could mean the product of a single number.

Consider $k+1$, if $k+1$ is a prime then $k+1$ can be written as a product of itself, as a product of one single prime.
Else, if $k+1$ is not a prime, then $\exists 1 < m, n < k+1 \ s.t. \ k+1 = mn$.
By induction hypothesis of strong induction, m, n can both be written as product of primes.
$m = \prod_{i=1}^{\ell} p_i, \ n = \prod_{i=1}^{t} q_i$ where p_i, q_i are all primes.
and $k+1 = \prod_{i=1}^{t} q_i \prod_{i=1}^{\ell} p_i$
thus $k+1 \in S$
by principle of strong induction, $\{2, 3, \dots, \} \subseteq S$. ∎

Theorem 3.2. There is no largest prime number.

Proof. (By contradiction)
Assume there is a largest prime p,
then $\{2, 3, 5, \cdots, p\}$ is the set of all primes
Let $M := (2 * 3 * 5 * \cdots * p) + 1 \in \mathbb{N}$
M is either prime or not.
Suppose M is not a prime, then by Lemma 3.1, $\exists p'$ dividing M.
Obviously $\forall i \in \{2 * 3 * 5 * \cdots * p\}, \ i \not| M$.
There is no prime dividing M, which contradict Lemma 3.1
Thus M is a prime, and $M > p$, which contradicts assumption
Therefore there is no largest prime. ∎

4 Lecture 4 Sep. 14 2018

Theorem 4.1 (the Fundamental Theorem of Arithmetic)**.** Every natural (except 1) is a product of prime(s), and the prime(s) in the product are unique including multiplicity except for the order.

Proof. We have already proven that the existential parts of this theorem in Lemma 3.1.
(Proof for the uniqueness part) Suppose there exists natural number (not 1) has 2 different prime factorizations.
By well ordering principle, there is a smallest n, which has two distinct prime factorizations.
Say $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ where p_i, q_i are all primes.
Notice that $p_i \neq q_j$ for any combination of (i, j) since if so $\frac{n}{p_i} = \frac{n}{q_j}$ is a natural number smaller than n having 2 distinct prime factorization, which contradicts our assumption above.
Specifically, $p_1 \neq q_1$.

(Case 1: $p_1 < q_1$)
Let $m := n - p_1 q_2 \dots q_\ell \in \mathbb{N}$
Notice $m = p_1(p_2 p_3 \dots p_k - q_2 q_3 \dots q_\ell)$
Also $m = (q_1 - p_1)(q_2 q_3 \dots q_\ell)$
$\implies m = p_1 \dots p_k = q_2 q_3 \dots q_\ell (q_1 - p_1)$
$\implies p_1 | m$ also notices that $p_1 \not| \, q_2 q_3 \dots q_\ell$
$\implies p_1 | (q_1 - p_1) \implies p_1 | q_1 \implies p_1 = q_1$
Contradicts the assumption that $p_q < q_1$
The other case goes a similar proof. ■

Definition 4.1. A natural number n is called **composite** if it's not 1 or a prime number.

Remark 4.1. Natural numbers are partitioned into 3 categories, 1, prime and composite numbers.

Example 4.1. Find 20 consecutive composite numbers.

$$(21!) + 2, (21!) + 3, \dots, (21!) + 21$$

Example 4.2. Find k consecutive composite numbers.

$$(k + 1!) + 2, (k + 1)! + 3, \dots, (k + 1!) + k + 1$$

5 Lecture 5 Sep. 17 2018

Definition 5.1. Let $a, b \in \mathbb{Z}$, and let $m \in \mathbb{N}$. If $m | a - b$ then we say "a and b are congruent modulo m"

Remark 5.1. Regular Induction $\iff$ Complete Induction $\iff$ Well-Ordering Principle

Proof. (WTS: Complete Induction $\implies$ Well-Ordering Principle)
Let $S \subseteq \mathbb{N}$ and $S \neq \emptyset$
(WTS, S has the smallest element)
Assume S does not have the smallest element.
Let $T := S^c$
Clearly $1 \in T$ (prop 1)
Since other wise 1 could be the smallest element of S.
Let $k \in \mathbb{N}$.
Suppose $1, 2, 3, \dots, k \in T$, if $k + 1 \notin T$, then $k + 1 \in S$ and $k + 1$ becomes the smallest element of S and contradicts our assumption above.

Therefore $1, 2, 3, \ldots k \in T \implies k+1 \in T$.
By principle of strong induction, $T = \mathbb{N}$.
Thus, $S = \emptyset$, and contradicts our definition of S.
Therefore $\forall S \subseteq \mathbb{N}$ *s.t.* $S \neq \emptyset$, S has the smallest element (Well-Ordering Principle). ■

Example 5.1 (Application 2)**.** Is $2^{29} + 3$ divisible by 7?

Solution. Notice $2^2 \equiv 4 \mod 7$ and $2^3 \equiv 1 \mod 7$.
$\implies (2^3)^9 \equiv 1^9 \mod 7$
$\implies 2^{27} \equiv 1 \mod 7$
$\implies 2^{29} \equiv 4 \mod 7$
Also $3 \equiv 3 \mod 7$
$\implies 2^{29} + 3 \equiv 4 + 3 \mod 7$
$\implies 2^{29} + 3 \equiv 7 \mod 7$
$\implies 7 | 2^{29} + 3$. ■

Theorem 5.1 (Rules on computing congruence)**.** Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

1. $a \equiv b \mod m \wedge c \equiv d \mod m \implies a + c \equiv b + d \mod m$
2. $a \equiv b \mod m \wedge c \equiv d \mod m \implies ac \equiv bd \mod m$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$,
suppose $a \equiv b \mod m \wedge c \equiv d \mod m$
by definition of congruence, $\exists p, q \in \mathbb{Z}$ *s.t.* $(a - b) = pm \wedge (c - d) = qm$
$\implies (a + c - b - d) = (p + q)m, \ (p + q) \in \mathbb{Z}$
$\implies a + c \equiv b + d \mod m$
And $a = b + pm \wedge c = d + qm$
$ac - bd = (b + pm)(d + qm) - bd$
$= bd + dpm + qbm + pqm^2 - bd$
$= (dp + qb + pqm)m$
$\implies m | ac - bd$
$\implies ac \equiv bd \mod m$ ■

Proposition 5.1 (Corollary from theorem 5.1)**.**

$$a \equiv b \mod m \implies a + c \equiv b + c \mod m$$

and

$$a \equiv b \mod m \implies a^k \equiv b^k \mod m, \ \forall k \in \mathbb{Z}_{\geq 0}$$

6 Lecture 6 Sep. 19 2018

Theorem 6.1. Let $a, b \in \mathbb{Z}$,

$$a = b \implies a \equiv b \mod m \; \forall m \in \mathbb{N}$$

Example 6.1. What is the reminder when $3^{202} + 5^9$ is divided by 8

Solution. Notice $3^2 \equiv 1 \mod 8$
Therefore, $(3^2)^{101} \equiv 1^{101} \mod 8$
That's, $3^{202} \equiv 1 \mod 8$
Also $5^2 \equiv 1 \mod 8$
$\implies (5^2)^4 \equiv 1^4 \mod 8$
$\implies 5^9 \equiv 5 \mod 8$
$\implies 3^{202} + 5^9 \equiv 5 + 1 \mod 8$
$\implies$ the reminder is 6.
(Notice that $3^{202} + 5^9 \equiv 6 \equiv 14 \equiv 22 \equiv \dots \mod 8$, and the reminder is the smallest integer satisfying above relation.) ■

Theorem 6.2. Let $M \in \mathbb{Z}$ and $M = d_N \dots d_2 d_1 d_0, \; d_i \in \{0, 1, \dots, 9\}$ [2], then

$$3 | M \iff 3 \mid \sum_{i=0}^{N} d_i$$

Proof. Notice $10 \equiv 1 \mod 3$, $100 \equiv 1 \mod 3$ and so on,
(Fact) $10^k \equiv 1 \mod 3, \; \forall k \in \mathbb{Z}_{\geq 0}$
Then $d_i 10^i \equiv d_i \mod 3, \; \forall i$
Therefore, $\sum_{i=0}^{N} 10^i d_i \equiv \sum_{i=0}^{N} d_i \mod 3$
Therefore $\sum_{i=0}^{N} 10^i d_i \equiv 0 \mod 3 \iff \sum_{i=0}^{N} d_i \equiv 0 \mod 3$

■

Theorem 6.3. Let $M \in \mathbb{Z}$ and $M = d_N \dots d_2 d_1 d_0, \; d_i \in \{0, 1, \dots, 9\}$, then

$$11 | M \iff 11 \mid \sum_{i=0}^{N} (-1)^i d_i$$

Proof. Notice $10^i \equiv (-1)^i \mod 11$
Therefore $10^i d_i \equiv (-1)^i d_i$
Thus, $\sum_{i=0}^{N} 10^i d_i \equiv \sum_{i=0}^{N} (-1)^i d_i \mod 11$
Then, $\sum_{i=0}^{N} 10^i d_i \equiv 0 \mod 11 \iff \sum_{i=0}^{N} (-1)^i d_i \equiv 0 \mod 11$

■

[2] This means the integer M is constructed from digits d_i. For example, $M = 256$, then $d_0 = 6, d_1 = 5, d_2 = 2$

7 Lecture 7 Sep. 21 2018

Theorem 7.1. Suppose p is a prime and $a, b \in \mathbb{N}$, if $p|ab$ then $p|a \vee p|b$.

Proof. If $a = 1 \vee b = 1$, then done. And for the case $a = b = 1$, the proposition is vacuously true.
Let $a, b > 1$,
By the fundamental theorem of arithmetic, we can write a, b as their unique prime factorization
$a = p_1^{\alpha_1} \dots p_k^{\alpha_k},\ \alpha_j \geq 1$ and $b = q_1^{\beta_1} \dots q_\ell^{\beta_\ell},\ \beta_j \geq 1$
then $ab = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_\ell^{\beta_\ell}$ is the unique prime factorization of ab.
Since $p \in \mathbb{P}$, therefore, $p = p_j \vee p = q_j \implies p|a \vee p|b$

■

Remark 7.1. We have shown that $a \equiv b \mod m \implies ca \equiv cb \mod m$. But notice that

$$ca \equiv cb \mod m \not\Longrightarrow a \equiv b \mod m$$

Definition 7.1. Let $a, b \in \mathbb{Z}$, then we say a and b are **relatively prime** if they have no prime factor in common.

Theorem 7.2. Suppose <u>p is a prime</u> and $a \in \mathbb{Z}$ and $p \nmid a$, then $ax \equiv ay \mod p \implies x \equiv y \mod p$.

Proof. Let $x, y, a \in \mathbb{N}$ and $p \in \mathbb{P}$.
Suppose $ax \equiv ay \mod p$
Then $p|a(x - y)$
By theorem 7.1, $p|a \vee p|(x - y)$
But by our assumption, $p \nmid a$, therefore $p|(x - y)$
Thus $x \equiv y \mod p$

■

Theorem 7.3 (Generalization of Theorem 7.2)**.** Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ and a and m are relatively prime. Then

$$ax \equiv ay \mod m \implies x \equiv y \mod m$$

Proof. Suppose $ax \equiv ay \mod m$
Then $m|a(x - y)$
Therefore $m|a \vee m|(x - y)$
For m to divide a, all of $m's$ prime factors have to be in the prime factorization of $|a|$.

But m and a are relatively prime, therefore $m \not| a$.
Therefore $m|(x-y)$ and that's $x \equiv y \mod m$

■

Theorem 7.4. Any integer a is congruent to mod m to exactly one of $\{0, 1, \ldots, m-1\}$.

Theorem 7.5 (Fermat's Little Theorem)**.** If p is a prime and $p \not| a$ (i.e. a and p are relatively prime), then

$$a^{p-1} \equiv 1 \mod p$$

Proof. Let $S := \{a1, a2, \ldots a(p-1)\}$
Notice that if $ax_i \equiv ax_j \mod p$, since $p \not| a$, $x_1 \equiv x_2 \mod p$.
Since $1 \leq x_i, x_j \leq p-1$, then $x_i = x_j$.
Therefore all elements in S are distinct with mod p
i.e. $x_i \not\equiv x_j \mod p$, $\forall (i,j) \in \mathbb{Z}^2$.
Since $p \not| a \land p \not| m$, $\forall m \in \{1, 2, \ldots, (p-1)\}$
So no element in S is congruent to $0 \mod p$.
Thus, S contains $p-1$ numbers and no two of them are congruent mod p.
Also none of them are congruent to $0 \mod p$.
By theorem 7.4, each element in S is congruent to one corresponding element in set $\{1, 2, \ldots, p-1\}$.
Therefore $(a1)(a2)\ldots(a(p-1)) \equiv 1 * 2 * \cdots * (p-1) \mod p$
That's $a^{p-1}(1 * 2 * \cdots * (p-1)) \equiv 1 * 2 * \cdots * (p-1) \mod p$
Clearly $p \not| (1 * 2 * \ldots (p-1))$, since if a prime divides a product of natural numbers, the prime must divide at least one of elements in the product.
Therefore $a^{p-1} \equiv 1 \mod p$

■

8 Lecture 8 Sep. 24 2018

Definition 8.1. Let $p \in \mathbb{N}$ and $a \in \mathbb{Z}$. The **multiplicative inverse** mod p of a is an integer b such that

$$ab \equiv 1 \mod p$$

Remark 8.1. Notice that the multiplicative inverse is generally not unique but unique up to mod p.

Corollary 8.1. Let $p \in \mathbb{P}$, $a \in \mathbb{N}$ and $p \not| a$. Then

$$\exists b \in \mathbb{Z},\ s.t.\ ba \equiv 1 \mod p$$

Proof. Let $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$
Suppose $p \nmid a$, then by Fermat's little theorem,
$a^{p-1} \equiv 1 \mod p \implies a^{p-2}a \equiv 1 \mod p$
Take $b = a^{p-2} \in \mathbb{Z}$ and $ab \equiv 1 \mod p$ ■

Example 8.1. Let $a = 8$ and $p = 5$. Obviously $p \nmid a$. By corollary above,

$$\exists b \in \mathbb{Z},\ s.t.\ 8b \equiv 1 \mod 5$$

Notice $b = 2$ satisfies above equation.

Remark 8.2. Corollary 8.1 requires p to be a prime.

Corollary 8.2 (Generalization)**.** Let a and $m \in \mathbb{N}$ and a and m are <u>relatively prime</u>, then

$$\exists b \in \mathbb{Z},\ s.t.\ ab \equiv 1 \mod m$$

Theorem 8.1 (Wilsons' Theorem)**.** Let $p \in \mathbb{P}$ then

$$(p-1)! \equiv -1 \mod p$$

Proof. Let $p \in \mathbb{P}$
if $p = 2 \vee p = 3$, then $1! \equiv -1 \mod 2$ and $2! \equiv -1 \mod 3$.
Otherwise, suppose $p > 3$,
Consider, let $S := \{2, 3, 4, \dots, p-2\}$
Notice that none of S is divisible by p.
Therefore p is relatively prime to all elements in S.
Then by Corollary 8.1, $\exists b_i \in \mathbb{Z}\ s.t.\ b_i s_i \equiv 1 \mod p,\ \forall s_i \in S$.
Notice that 0 has no multiplicative inverse and

$$(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \mod p$$

That's, 1 and $(p-1)$ have themselves as their multiplicative inverse.
Also notice that for any $s_i \in S$, s_i does not have itself as its multiplicative inverse.
If $a \in S$ has itself as it's multiplicative inverse, then

$$\begin{aligned} a^2 &\equiv 1 \mod p \\ \implies a^2 - 1 &\equiv 0 \mod p \\ \implies (a+1)(a-1) &\equiv 0 \mod p \\ \implies p &| (a+1)(a-1) \end{aligned}$$

Notice that at last one of $(a+1)$ and $(a-1)$ is in set S since $p > 3 \implies S \neq \emptyset$.
This contradicts what we argued above, *none of S is divisible by p.*
That's

$$s_i s_i \not\equiv 1 \mod p, \ \forall s_i \in S$$

Note that if y is a multiplicative inverse of x, then x is a multiplicative inverse of y.
Notice that for any $s_i \in S$, by Corollary 8.1,
there exists an integer b_i s.t. $s_i b_i \equiv 1 \mod p$
And the multiplicative inverse is unique up to $\mod p$,
Thus $s_i(b_i \mod p) \equiv 1 \mod p$ and $(b_i \mod p) \in S$.
And for all elements in S has one of their multiplicative inverse in S,
That's

$$s_i s_j \equiv 1 \mod p, \ i \neq j$$

Notice $p > 3$ implies p is odd, so $|S|$ is even.
Match every pair of multiplicative inverses in S and they collapse to 1 $\mod p$
Therefore

$$\begin{aligned} 2 \cdot 3 \cdot 4 \cdots (p-2) &\equiv 1 \mod p \\ \implies 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1) &\equiv (p-1) \mod p \\ \implies (p-1)! &\equiv -1 \mod p \end{aligned}$$

■

9 Lecture 9 Sep. 26 2018

Remark 9.1. Recall that an integer n is even iff $n \equiv 0 \mod 2$ and is odd iff $n \equiv 1 \mod 2$.

Theorem 9.1. There are infinitely many primes of the form $4k+3$, where $k \in \mathbb{Z}$.

Proof. Note that odd numbers n can be classified as $n \equiv 1 \mod 4$ and $n \equiv 3 \equiv -1 \mod 4$
(Suppose 1) there are only finitely many primes in the form $4k+3$.
Let finite set $S := \{p_1, p_2, \ldots p_m\}$ denotes the collection of them.
And notice that $p_i \equiv -1 \mod 4, \ \forall p_i \in S$.
Let

$$M := (p_1 \cdot p_2 \cdots p_m)^2 + 2$$

and $M \equiv 1 + 2 \equiv 3 \equiv -1 \mod 4$.
Therefore M is an odd natural number.
By the Fundamental Theorem of Arithmetic, M can be factorized into product of primes.

$$M = \prod_{i=1}^{\ell} q_i$$

and since M is odd, $q_i \neq 2 \ \forall\ i$. Thus all q_i are odd.
(Suppose 2) All $q_i \equiv 1 \mod 4$.
Then $M \equiv 1 \mod 4$.
Contradict the fact that $M \equiv -1 \mod 4$. Thus (Suppose 2) is false.
Therefore $\exists i,\ s.t.\ q_i \equiv -1 \mod 4$.
From (Suppose 1), S is the collection of all primes that $\equiv -1 \mod 4$.
Therefore $q_i = p_j$ for some j.
Therefore $p_j | M$.
Also note that $p_j | (p_1 \cdot p_2 \cdots p_m) \implies p_j | (p_1 \cdot p_2 \cdots p_m)^2$
$\implies p_j | 2 \implies p_j = 2$ contradicts the fact that p_j is odd.
Therefore (Suppose 1) is false, there are infinitely many primes taking the form $4k + 3$.

■

Example 9.1. Find $7^{20^{30}} \mod 5$.

Solution. Let $n := 20^{30}$.
Notice that $7^4 \equiv 1 \mod 5$.
And if $n \equiv r \mod 4$ where $r \in \mathbb{Z}$,
$n = 4k + r$ and $7^n \equiv 7^{4k+r} \equiv (7^4)^k \times 7^r \equiv 1^k \times 7^r \equiv 7^r \mod 5$.
Notice that $20 \equiv 0 \mod 4 \implies 20^{30} \equiv 0 \mod 4$.
Thus $r = 0$.
Therefore $7^n \equiv 7^0 \equiv 1 \mod 5$.
Thus $7^{20^{30}} \mod 5 = 1$. ■

Example 9.2. Find $10^{3^{30}} \mod 7$.

Solution. Notice that $10^6 \equiv 1 \mod 7$.
And $3 \equiv 3 \mod 6, 3^2 \equiv 3 \mod 6, 3^3 \equiv 3 \mod 6 \ldots$
Using induction, we can show that

$$3^k \equiv 3 \mod 6,\ \forall k \in \mathbb{Z}_{\geq 0}$$

Therefore $3^{30} \equiv 3 \mod 6$.
That's $3^{30} = 6k + 3$ for some k.
Thus $10^{3^{30}} \equiv (10^6)^k \times 10^3 \equiv (1)^k \times 10^3 \equiv -1 \equiv 6 \mod 7$.
So $10^{3^{30}} \mod 7 = 6$.

$\blacksquare$