The purpose of this document is to collect the central results which we have discussed. Of course, it should be noted that Missions 1,2 and 3 give some indication of what the test is likely to focus upon. Modulo bonus problems naturally, that said, there may still be sub-calculations in the bonus problems which are worth study. For example, solving $f(x) = x^{18} + x^{14} + 3x + 10 \equiv 0$ modulo 21 is a **pain**, but, is $f(4) \equiv 0$ modulo 21 is a completely reasonable test question.

Notation matters. Please take some time to have a clear mind about what is meant by $[a] = [b]$ verses $a \equiv b$ modulo n. I usually give you freedom to work with equality of sets or with congruence of integers. But, you ought to be aware the difference.

1 definitions and theorems

Theorem 1.1. nonzero division algorithm: *If $a, b \in \mathbb{Z}$ with $b \neq 0$ then there is a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ for which*

$$a = qb + r \qquad \& \qquad 0 \leq r < |b|.$$

Definition 1.2. *Let $a, b \in \mathbb{Z}$ then we say b **divides** a if there exists $c \in \mathbb{Z}$ such that $a = bc$. If b divides a then we also say b is a **factor** of a and a is a **multiple** of b.*

The notation $b \mid a$ means b divides a. If b is does not divide a then we write $b \nmid a$.

Definition 1.3. *If $p \in \mathbb{N}$ such that $n \mid p$ implies $n = p$ or $n = 1$ then we say p is **prime**.*

In words: a prime is a positive integer whose only divisors are 1 and itself.

Proposition 1.4. *Let $a, b, c, d, m \in \mathbb{Z}$. Then,*

- **(i.)** *if $a \mid b$ and $b \mid c$ then $a \mid c$,*
- **(ii.)** *if $a \mid b$ and $c \mid d$ then $ac \mid bd$,*
- **(iii.)** *if $m \neq 0$, then $ma \mid mb$ if and only if $a \mid b$*
- **(iv.)** *if $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.*

Theorem 1.5. *Let $a_1, \dots, a_k, c \in \mathbb{Z}$. Then,*

- **(i.)** *if $c \mid a_i$ for $i = 1, \dots, k$ then $c \mid (u_1a_1 + \cdots + u_ka_k)$ for all $u_1, \dots, u_k \in \mathbb{Z}$,*
- **(ii.)** *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Corollary 1.6. *If $c \mid x$ and $c \mid y$ then $c \mid (ax + by)$ for all $a, b \in \mathbb{Z}$.*

Definition 1.7. *If $d \mid a$ and $d \mid b$ then d is a* **common divisor** *of a and b. Moreover, if $a, b \in \mathbb{Z}$, not both zero, then the* **greatest common divisor** *of a and b is denoted $gcd(a, b)$.*

Lemma 1.8. *Let $a, b, q, r \in \mathbb{Z}$. If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$.*

This Lemma leads quickly to the Euclidean algorithm below:

Theorem 1.9. Euclidean Algorithm: *suppose $a, b \in \mathbb{N}$ with $a > b$ and form the finite sequence $\{b, r_1, r_2, \dots, r_n\}$ for which $r_{n+1} = 0$ and $b, r_1, \dots, r_n$ are defined as given by the division algorithm:*

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \dots, \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Then $gcd(a, b) = r_n$.

In addition to mere calculation of $gcd(a, b)$ the Euclidean algorithm provides the following[1]:

Theorem 1.10. Bezout's Identity: *if $a, b \in \mathbb{Z}$, not both zero, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.*

In what follows, we assume $n \in \mathbb{N}$ throughout.

Definition 1.11. *Let $a, b \in \mathbb{Z}$ then we say a is* **congruent** *to b $mod(n)$ and write $a \equiv b$ $mod(n)$ if a and b have the same remainder when divided by n.*

The definition above is made convenient by the simple equivalent criteria below:

Theorem 1.12. *$a \equiv b$ $mod(n)$ if and only if $n \mid (b - a)$.*

Proposition 1.13. *Let n be a positive integer, for all $x, y, z \in \mathbb{Z}$,*

(i.) *$x \equiv x$ $mod(n)$,*

(ii.) *$x \equiv y$ $mod(n)$ implies $y \equiv x$ $mod(n)$,*

(iii.) *if $x \equiv y$ $mod(n)$ and $y \equiv z$ $mod(n)$ then $x \equiv z$ $mod(n)$.*

Corollary 1.14. *Let $n \in \mathbb{N}$. Congruence modulo n forms an equivalence relation on $\mathbb{Z}$.*

Definition 1.15. equivalence classes of $\mathbb{Z}$ modulo $n \in \mathbb{N}$:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\}$$

[1] calculationally this is accomplished by manipulation of the vector (a, b) to shadow the algorithm as we saw in the last Episode

Observe, there are several ways to characterize such sets:

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \ mod(n)\} = \{y \in \mathbb{Z} \mid y - x = nk \text{ for some } k \in \mathbb{Z}\} = \{nk + x \mid k \in \mathbb{Z}\}.$$

I find the last presentation of $[x]$ to be useful in practical computations.

Definition 1.16. Coset Notation: *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ we define:*

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \qquad n\mathbb{Z} + a = \{nk + a \mid k \in \mathbb{Z}\}.$$

Observe, in the notation just introduced, we have

$$\boxed{[a] = n\mathbb{Z} + a}$$

Equivalence classes of an equivalence relation are disjoint. Therefore, the proposition below is an inevitability:

Proposition 1.17. *Let $n \in \mathbb{N}$. We have $[x] = [y]$ if and only if $x \equiv y \ mod(n)$. Or, in the coset notation $n\mathbb{Z} + x = n\mathbb{Z} + y$ if and only if $y - x \in n\mathbb{Z}$.*

In contrast to the proposition above, the one that follows is not generally true for other equivalence relations where there might not even exist some concept of $+$ or $\times$.

Proposition 1.18. *Let $n \in \mathbb{N}$. If $[x] = [x']$ and $[y] = [y']$ then*

(i.) $[x + y] = [x' + y']$,

(ii.) $[xy] = [x'y']$

(iii.) $[x - y] = [x' - y']$

Of course, we sometimes find it convenient to think in terms of congruences:

Corollary 1.19. *Let $n \in \mathbb{N}$. If $x \equiv x'$ and $y \equiv y'$ modulo n then*

(i.) $x + y \equiv x' + y' \ mod(n)$,

(ii.) $xy \equiv x'y' \ mod(n)$,

(iii.) $x - y \equiv x' - y' \ mod(n)$,

Definition 1.20. modular arithmetic: *let $n \in \mathbb{N}$, define*

$$[x] + [y] = [x + y] \qquad \& \qquad [x][y] = [xy]$$

for all $x, y \in \mathbb{Z}$. Or, if we denote the set of all equivalence classes modulo n by $\mathbb{Z}/n\mathbb{Z}$ then write: for each $n\mathbb{Z} + x, n\mathbb{Z} + y \in \mathbb{Z}/n\mathbb{Z}$

$$(n\mathbb{Z} + x) + (n\mathbb{Z} + y) = n\mathbb{Z} + x + y \qquad \& \qquad (n\mathbb{Z} + x)(n\mathbb{Z} + y) = n\mathbb{Z} + xy.$$

Finally, we often use the notation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Notice many properties of integer arithmetic transfer to $\mathbb{Z}/n\mathbb{Z}$, for $k \in \mathbb{N}$,

$$[a_1] + [a_2] + \cdots + [a_k] = [a_1 + a_2 + \cdots + a_k]$$
$$[a_1][a_2]\cdots[a_k] = [a_1 a_2 \cdots a_k]$$
$$[a]^k = [a^k].$$

Naturally, as we discuss $\mathbb{Z}_n$ it is convenient to have a particular choice of representative for this set of residues. Two main choices: the *set of least non-negative residues*

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

alternatively, *set of least absolute value residues* or simply *least absolute residues*

$$\mathbb{Z}_n = \{[0], [\pm 1], [\pm 2], \ldots\}$$

where the details depend on if n is even or odd.

Sorry folks, out of time for more here, basically, what I fail to list here are the theorems from Lecture 4. In particular, Fermat's little theorem, Lagrange's Theorem and Euler's Theorem. I do hope you know these and I wouldn't be too surprised if I asked for a proof of something in that lecture.

Theorem 1.21. Prime Divisor Property: *If a prime $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof: see Lecture 2.

Theorem 1.22. Unique Prime Factorization of $\mathbb{N}$: *Let $n \in \mathbb{N}$ then there exist a unique set of distinct primes $p_1, p_2, \ldots, p_k$ and multiplicities $r_1, r_2, \ldots, r_k$ for which $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$.*

Proof: see Lecture 2.

Theorem 1.23. Prime Factorization of squares: *there exists $m \in \mathbb{N}$ such that $n = m^2$ iff n is the product of primes to even powers.*

Proof: this is essentially a corollary to the unique prime factorization theorem.

Theorem 1.24. Square coprime products: *if $gcd(a, b) = 1$ and $ab = m^2$ for some $m \in \mathbb{N}$ then there exist $j, k \in \mathbb{N}$ such that $a = j^2$ and $b = k^2$. Moreover, a coprime product is a square iff it is the product of squares.*

Proof: notice the product of squares is a square hence the forward implication is the only nontrivial assertion in the above theorem.

Theorem 1.25. Irrationality of square root: *if N is a non-square natural number then $\sqrt{N}$ is irrational.*

Proof: see Lecture 2 page 7.

Theorem 1.26. Product of gcd and lcm: *let $a, b \in \mathbb{N}$ then $ab = gcd(a, b)lcm(a, b)$.*

Proof: see page 33 of Stillwell.

Theorem 1.27. *Let $n \in \mathbb{N}$ such that there exist a unique set of distinct primes $p_1, p_2, \dots, p_k$ and multiplicities $r_1, r_2, \dots, r_k$ for which $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Then $a \equiv b \ mod(n)$ if and only if $a \equiv b \ mod(p_i^{r_i})$ for each $i = 1, 2, \dots k$.*

Proof: see Episode I.

Theorem 1.28. *Let $f(x) \in \mathbb{Z}[x]$, that is let $f(x)$ be a polynomial with integer coefficients, and suppose $n \in \mathbb{N}$. If $a \equiv b \ mod(n)$ then $f(a) \equiv f(b) \ mod(n)$.*

Proof: see Episode I.

Theorem 1.29. General Solution of the Linear Diophantine Equation: *If $a, b, c \in \mathbb{Z}$ then $ax + by = c$ has an integer solution iff $gcd(a, b) \mid c$. Furthermore, supposing $d = gcd(a, b)$ there exist $m, n \in \mathbb{Z}$ such that $d = am + bn$. All integer solutions of $ax + by = c$ are hence constructed: for each $t \in \mathbb{Z}$,*

$$x = md + \frac{bt}{d} \qquad \& \qquad y = nd - \frac{at}{d}.$$

Proof: see Lecture 2.

2 standard problems

(1.) find the least positive residue of a^x mod n where x is stupidly large.

(2.) calculate $\phi(n)$ for some $n < 500$. (I think you guys can find prime factorizations of integers less than 500 with relative ease, do have a calculator, notice there must be a prime factor $p < \sqrt{500}$ so you only have about 20 things to check, many of which are immediately ruled out for a given n)

(3.) solve $ax \equiv b$ modulo n if possible.

(4.) test if $a, b \in \mathbb{Z}$ are relatively prime. If so, exhibit Bezout's Identity.

(5.) simplify things with respect to modular arithmetic.

(6.) Find multiplication table for $(\mathbb{Z}/k\mathbb{Z})^{\times}$. In the case k is prime this is quite easy, in the case k is composite it requires some thought.

(7.) Find the order of a given element in $(\mathbb{Z}/k\mathbb{Z})^{\times}$

(8.) Is it possible a particular element in $(\mathbb{Z}/k\mathbb{Z})^{\times}$ has order blah? (what theorem helps here?)

(9.) Find cosets with respect to particular subgroup of $(\mathbb{Z}/k\mathbb{Z})^{\times}$.

(10.) Find binary, or other base, representation of a given positive integer.

(11.) Binary exponentiation: can use calculate $[m]^{347}$ modulo 37 without taking the whole test time? What is your strategy of attack on such a problem? (see page 7 of Lecture 7 for the idea, you don't have to adhere to my exact method, but, be aware the concept)

(12.) prove your basic divisibility lemmas

(13.) use prime factorization theorems to prove irrationality of $\sqrt{n}$ with ease. (in contrast, in another course, you might use the well-ordering-principle on some particular set, this semester we took a more constructive approach. This comment mostly for those of you who studied with Kester or happen to recall how you proved $\sqrt{2}$ was irrational in Math 200 by arguments not based on direct application of the fundamental theorem of arithmetic.

(14.) what is the fundamental theorem of arithmetic? (I may have failed to say this in class, for shame!)

(15.) show $f(x) = 0$ permits no integer solutions via appropriate modular arithmetic. (here, to be kind, your instructor should pick $f(x)$ for which $f(x) \not\equiv 0$ modulo n for say $n = 2, 3, 4, 5$)

(16.) Chinese remainder problem (with relatively prime moduli)

(17.) Egyptian fraction finding

(18.) Continued fraction finding

(19.) Casting out whatever type problems (see lecture 3 for the flavor)

(20.) (Removed from test 1: we actually do more justice to this soon after test 1.) Be able to prove the 2-square identity (can use complex number if you like, or just direct algebra if you insist on keeping it real).

(21.) (Removed from test 1: we actually do more justice to this soon after test 1.) Be able to verify Euclid's parametric formulas for Pythagorean triples.

(22.) can you prove the prime divisor property?