Notes for Test 2

There will be **six** problems on Test 2. Each problem will be worth **20** points. The first problem will be **10** Truth-False questions.
The test will cover Divisibility (2.3), prime factorization and greatest common divisor (2.4) and from Groups (3.1) and (3.2).

For example that $(ab)^{-1} = a^{-1}b^{-1}$ yields commutativity is a typical test problem In general $(ab)^{-1} = b^{-1}a^{-1}$. But we are given that
$b^{-1}a^{-1} = a^{-1}b^{-1}$. Now we take the inverse on both sides and get
$(b^{-1}a^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab$, and $(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$.
Thus $ba = ab$.
The problem on the test will be very similar. Do problem 15, page 160

One main example of a group is the group of integers modulo k. This material is somewhat spread out in the book. Here is what you need to know.

Integers modulo k

This is section 2.5 in the book. It combines what you learned about equivalence relations together with the definition of groups:
For every integer n and $k > 0$ we have division of n by k with remainder

$$n = qk + r, 0 \leq r < k$$

We say that n and m are *congruent modulo* k if in the divsion algorithm for n and m both numbers divided by k have the same remainder. This partitions the set $\mathbb{Z}$ of integers into k equivalence classes, namely in classes where the remainder is $r = 0, r = 1, \ldots, r = k - 1$
Examples: Let $k = 2$. The possible remainders are $r = 0$ and $r = 1$. Numbers n and m have remainder $r = 0$ only if they are **both even** and remainder $r = 1$ if they are **both odd**. Thus the class $[0]$ of 0 is the set of all even numbers, the class $[1]$ of 1 is the set of all odd numbers. Because we are talking congruence modulo 2, we use a subscript 2 :
$[0]_2 = \{\ldots -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, \ldots\}$, and $[1]_2 =$
$\{\ldots -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, \ldots\}$
Let $k = 3$. According to possible remainders $r = 0, r = 1, r = 2$ we get three classes:
$[0]_3 = \{\ldots -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}, [1]_3 = \{\ldots -14, -11, -8, -5, -2, 1, 4, 7, 10, 13$
$[2]_3 = \{\ldots -13, -10, -7, -4, -1, 2, 5, 7, 10, \ldots\}$

Theorem. *For* $k > 0$ we have

$$[n]_k = n + k\mathbb{Z} = \{n + kx | x \in \mathbb{Z}\}$$

Proof. If n and m are in the same class then both numbers have the same remainder r, where $0 \leq r < k$,. That is

$$n = q_1 k + r, m = q_2 k + r$$

Thus

$$m = n + (q_2 - q_1)k$$

Hence,

$$[n]_k \subseteq n + k\mathbb{Z}$$

On the other hand, if $m = n + kx$ we have that $m - n = kx$. That is $m - n$ is divisible by k But according to the division algorithm we also have $m = q_2 k + r_2$ and $n = q_1 k + r_1$. If r_2 and r_1 are different then we may assume $r_2 > r_1$. We get

$$m - n = (q_2 - q_1)k - (r_2 - r_1)$$

We have that $m - n$ is divisible by k. On the right side $(q_2 - q_1)k$ is divisible by k. Thus $(r_2 - r_1)$ must be divisible by k. But this is impossible because $0 < r_2 - r_1 < k$.

For $k > 0$ we get exactly k congruence classes according to the possible remainders. The set of classes modulo k is denoted as $\mathbb{Z}_k$:

$$\mathbb{Z}_k = \{[0]_k, [1]_k, \ldots, [k-1]_k\}$$

$\mathbb{Z}_k$ is a set of k –many elements, where each element is a subset of $\mathbb{Z}$. Each $n \in \mathbb{Z}$ is congruent modulo k to exactly one r where $0 \leq r < k$.

$$[n]_k = [r]_k = r + k\mathbb{Z}$$

Theorem. **For every** $k > 0$ one has that the set $\mathbb{Z}_k$ is a commutative group of k –many elements:

$$[n]_k + [m]_k = [n+m]_k, -[n]_k = [-n]_k, 0 = [0]_k$$

Proof. The difficult part is to understand that we actually have defined operations. That is if $[n]_k = [n']_k$ and $[m]_k = [m']_k$ then $[n+m]_k = [n' + m']_k$. But this is quite obvious: n and m differ from n' and m' by a multiple of k. And therefore $n + m$ and $n' + m'$ differ by a multiple of k. (To be explicit: $n' = n + ks, m' = m + kt, n' + m' = n + m + k(s+t)$) Thus $[n+m]_k = [n' + m']_k$. We have a similar argument for taking the additive inverse and for the zero-element. Keep in mind that the zero of $\mathbb{Z}_k$ is $k\mathbb{Z}$.

That we get with these definitions a commutative group is easy to see. The group properties are inherited from the integers. Like associativity:
$([a] + [b]) + [c] = [a+b] + [c] = [(a+b)+c] = [a+(b+c)] = [a] + [b+c] = [a] + ([b] + [$
$[a] + [b] = [a+b] = [b+a] = [b] + [a]$
That $[0]$ is the zero for $\mathbb{Z}_k$ is also clear: $[a] + [0] = [a+0] = [a]$ and
$[a] + (-[a]) = [a] + [-a] = [a - a = 0]$

Example: $[8]_{12} + [7]_{12} = [15]_{12} = [3]_{12}$. But also: $[8]_{12} = [8 - 48 = -40]_{12}$, $[7]_{12} = [7 + 60 = 67]_{12}, [8]_{12} + [7]_{12} = [-40 + 67 = 27]_{12} = [3]_{12}$

We can also multiply elements of $\mathbb{Z}_k$ by the same rules:

$$[n]_k \cdot [m]_k = [nm]_k$$

One needs to show, if $[n] = [n'], [m] = [m']$ then $[nm] = [n'm']$. You should do this as an exercise.

Theorem. With respect to multiplication, $\mathbb{Z}_k$ is a commutative semigroup with unit $[1]_k$. We also have that multiplication is distributive over addition.

Proof. Commutativity: $[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]$;

Distributivity:

$[a] \cdot ([b] + [c]) \;\; = [a] \cdot ([b + c]) \;\; = [a(b + c)] \;\; = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$

Unit: $[a] \cdot [1] = [a1] = [a]$. Remember that $[1] = 1 + k\mathbb{Z} = \{1 + kl | l \in \mathbb{Z}\}$

Example: $[8]_{12} \cdot [7]_{12} = [56]_{12} = [8]_{12}$

This tells us that we don't have in $\mathbb{Z}_{12}$ the cancellation property: We have $[8] \cdot [7] = [8] \cdot [1] = [8]$. The reason is that not every element has an inverse.

Theorem. If $(m, k) = 1$ then $[m]_k$ has a multiplicative inverse in $\mathbb{Z}_k$.

Proof. We have $xm + yk = 1$. Therefore $[x][m] + [y][k] = [1]$ in $\mathbb{Z}_k$. However $[y][k] = [yk] = [0]$. Therefore $[x][m] = [1]$. We got that $[x]$ is the inverse of $[m]$.

Corollary. For every prime p one has that all classes $[1]_p, [2]_p, \ldots, [p - 1]_p$ have a multiplicative inverse.

Proof. we have $(a, p) = 1$ for $a = 1, 2, \ldots, p - 1$.

Example. $(7, 12) = 1$. By the theorem, $[7]_{12}$ must have an inverse. From $3 \cdot 12 - 5 \cdot 7 = 1$ we see that $[-5]$ is in $\mathbb{Z}_{12}$ the inverse of $[7]$. We also have $[-5] = [7]$. indeed $[7] \cdot [7] = [49] = [1]$ in $\mathbb{Z}_{12}$.

In $\mathbb{Z}_5$ all four classes different from 0 must have an inverse:

$[1]^{-1} = [1], [2]^{-1} = [3], [3]^{-1} = [2], [4]^{-1} = [4]$

As a further example we have $(11, 30) = 1$. We get that $11 \cdot 11 - 4 \cdot 30 = 1$ (do the calculations for $x11 + y30$) Therefore 11 has an inverse modulo 30, Namely $[11]^{-1} = [11]$.

We can solve something like

$x \cdot [11]_{30} = [8]_{30}$: $x = [8] \cdot [11]^{-1} = [8] \cdot [11] = [88] = [88 - 90] = [-2] = [28]$. Check: $[28] \cdot [11] = [308] = [10 \cdot 30 + 8] = [8]$