Homework 4 solutions.

Problem 11.2. Let H be a subgroup of a group G. Prove that $g_1H = g_2H$ if and only if $g_1^{-1}g_2$ belongs to H.

Proof. Suppose $g_1H = g_2H$. Since H is a subgroup, the identity e is in H. So $g_2 \in g_2H$. Since $g_1H = g_2H$, there is some element $h \in H$ s.t. $g_2 = g_1h$. Multiplying both sides by g_1^{-1} on the left, we get that $g_1^{-1}g_2 = h$. Since $h \in H$ we have $g_1^{-1}g_2 \in H$.

Suppose $g_1^{-1}g_2$ belongs to H. So for some $h \in H$, take an element $g_1h \in g_1H$. Note that if $g_1^{-1}g_2 \in H$ then its inverse, $g_2^{-1}g_1 \in H$. Thus the element $g_2^{-1}g_1h$ is also in H. Let $h' = g_2^{-1}g_1h$. Finally note that $h = (g_1^{-1}g_2)(g_2^{-1}g_1)h = (g_1^{-1}g_2)h'$. So $g_1h = g_2h'$. But g_2h' is by definition an element of g_2H. So every element of g_1H is also an element of g_2H. Since the labels g_1 and g_2 are arbitrary, the same argument also shows that every element of g_2H is also an element of g_1H. Therefore $g_1H = g_2H$. □

Problem 11.3. If H and K are finite subgroups of a group G, and if their orders are relatively prime, show that they have only the identity element in common.

Proof. Suppose H and K share an element x. Then the order of x divides the orders of both H and K. But since the orders of H and K are relatively prime, the only number that divides both their orders is 1. So x must have order 1. The only element of order 1 is e. So the only element H and K have in common is the identity. □

Problem 11.5. Given subsets X and Y of a group G, write XY for the set of all products xy where $x \in X$ and $y \in Y$. If X and Y are both finite, if Y is a subgroup of G, and if XY is contained in X, prove that the size of X is a multiple of the size of Y.

Proof. We showed in problem 11.2 that $x_1Y = x_2Y$ iff $x_1^{-1}x_2 \in Y$. We use this fact to show that two cosets x_1Y and x_2Y are either equal or disjoint. Suppose x_1Y and x_2Y are not disjoint. So there are elements $x_1y_1 \in x_1Y$ and $x_2y_2 \in x_2Y$ s.t. $x_1y_1 = x_2y_2$. But then $y_2^{-1}y_1 = x_1^{-1}x_2$. Since $y_2^{-1}y_1 \in Y$ we have that $x_1^{-1}x_2 \in Y$. Thus by problem 11.2, we have $x_1Y = x_2Y$.

X is a finite set, so let's list its elements. So $X = \{x_1, x_2, \dots, x_n\}$. Thus

$$XY = \bigcup_{i=1}^{n} x_iY$$

Any two sets x_iY, x_jY are either equal or disjoint. Furthermore, for $y \neq y' \in Y$, we have $x_iy \neq x_iy'$. So any set $x_iY$has the same number of elements as Y. Let $|Y| = m$. Then the number of elements in XY is some multiple of m.

Since Y is a subgroup, $e \in Y$. So we have that $Xe \subset XY$. That is, $X \subset XY$ for any set X and subgroup Y. We are given that $XY \subset X$. These two facts combined give us that $XY = X$. Since $XY = X$, and the number of elements in XY is some multiple of $|Y|$, we get that the size of X is a multiple of the size of Y. □

Problem 11.7. Let n be a positive integer, and let m be a factor of $2n$. Show that D_n contains a subgroup of order m.

Proof. The group D_n is generated by the rotation r which has order n and the reflection s which has order 2. Note that an element of the form r^l has order k where k is the smallest number for which kl is a multiple of n. And an element of the form sr^l has order 2. Recall also that if an element has order l then the smallest subgroup generated by that element also has order l.

Let m be a factor of $2n$. This means that either m divides n itself, or $m = 2m'$ and m' divides n.

Suppose first that m divides n. That is, $n = m * k$ for some integer k. Thus the subgroup generated by r^k has order m.

Now suppose $m = 2m'$ where m' divides n. Again, this means $n = m'k$ for some integer k. Consider the subgroup generated by r^k and s. This group has at least all m' powers of r^k of the form r^{kl} and all elements of the form sr^{kl}. Suppose we multiply two elements $s^\delta r^{kl}$ and $s^{\delta'} r^{kl'}$ where δ, δ' are either 0 or 1. If $\delta' = 1$, we get

$$(s^\delta r^{kl})(sr^{kl'}) = s^\delta r^{kl-kl'}$$

so this is another element of the form $sr^{kl''}$. If $\delta' = 0$ then $(s^\delta r^{kl})(r^{kl'}) = s^\delta r^{kl+kl'}$ which is also of that form. So all the element of the subgroup generated by r^k and s are either of the form r^{kl} or of the form sr^{kl}. There are m' distinct powers of r^k, and each power of r^k can also be multiplied by s. So there are exactly $2m' = m$ elements in this group. Therefore, for every integer m dividing $2n$ there is a subgroup of D_n of order m. $\square$

Problem. Compute the order of 2 in the multiplicative group mod 59.

Answer. The order of 2 divides the order of the group. The order of the group is the number of $n \in \mathbb{N}$ s.t. $n \leq 59$ and n and 59 are relatively prime. Since 59 is prime, there are 58 such numbers. So the order of 2 divides 58. The divisors of 58 are 1,2,29 and 58. The order of 2 is neither 1 nor 2, as neither 2 nor 4 equal 1 mod 59. So that leaves 29 or 58.

We can compute powers of 2 mod 59 by noting that $2^6 = 64 \equiv 5$ mod 59. So $2^{12} \equiv 25$ mod 59 giving that $2^{24} \equiv 35$ mod 59. Also, $2^4 = 32$. Thus $2^{29} = 2^5 \cdot 2^{24} \equiv 58$ mod 59. So the order of 2 is not 29. Therefore the order of 2 is 58. $\square$

Problem. Find an integer x such that x^{71} is congruent to 3 mod 1001.

Answer. We want to solve the equation $x^{71} \equiv 3$ mod 1001.

First we compute $\phi(1001)$. Note that $1001 = 7 \cdot 11 \cdot 13$. There are 1001 positive numbers n s.t. $n \leq 1001$. Of them, $11 \cdot 13$ are multiples of 7, $7 \cdot 13$ are multiples of 11, and $7 \cdot 11$ are multiples of 13. Of *those* numbers, 13 are multiples of both 7 and 11, then 11 are multiples of both 7 and 13, and finally, 7 are multiples of both 11 and 13. Only 1001 is a multiple of 7, 11 and 13. Thus $\phi(1001) = 1001 - 7 \cdot 11 - 7 \cdot 13 - 11 \cdot 13 + 7 + 11 + 13 - 1$. In all we get $\phi(1001) = 720$.

Note that for any number x, we have that $x^{720} \equiv 1$ mod 1001. Moreover, for any integer f, $x^{720f} \equiv 1$ mod 1001. In general, for any number k where $k \equiv k'$ mod 720, $x^k \equiv x^{k'}$ mod 1001. So if we find a number d for which $71d \equiv 1$ mod 720, we would get that $x^{71d} \equiv x$ mod 1001. Then we could just raise both sides of the equation $x^{71} \equiv 3$ to the d and get that x is 3^d mod 1001.

Thus we have to solve the equation $71 * d \equiv 1$ mod 720. This is the same as finding integers d and f s.t. $71d + 720f = 1$. One can find such a number using the Euclidean Algorithm. It goes

$$720 = 71 \cdot 10 + 10$$
$$71 = 10 \cdot 7 + 1$$

Since this means that $10 = 720 - 71 \cdot 10$, we get $71 = (720 - 71 \cdot 10) \cdot 7 + 1$. So $71 \cdot 71 - 720 \cdot 7 = 1$. Thus $d = 71$ (and $f = 7$).

So take the equation $x^{71} \equiv 3 \bmod 1001$. Raise both sides to the 71^{st} power. We get $x^{71 \cdot 71} \equiv 3^{71} \bmod 1001$. Since $71 \cdot 71 \equiv 1 \bmod 1001$, we get that $x \equiv 3^{71} \bmod 1001$. So $x = 3^{71}$.

We can compute $3^{71} \bmod 1001$. A calculator tells us that $3^8 = 6561 \equiv 555 \bmod 1001$. Taking successive squares we get that $3^{16} \equiv 718$, $3^{32} \equiv 9 \bmod 1001$. Then $3^{64} \equiv 81 \bmod 1001$. Finally, $3^7 \equiv 185 \bmod 1001$. So $3^{71} = 3^{64} \cdot 3^7 \equiv 971 \bmod 1001$. Therefore $x = 971 \bmod 1001$. $\square$