MATH 124 HOMEWORK #2

INNA ZAKHAREVICH

(1) Notice that $143 = 11 \cdot 13$. Considering the polynomial $x^3 - 9x^2 + 23x - 15$ modulo 11 we get

$$x^3 + 2x^2 + x - 4 = (x-1)(x^2 + 3x + 4).$$

The solution to the quadratic above is $\frac{-3 \pm \sqrt{-7}}{2} = 6(-3 \pm \sqrt{4}) = 6(-3 \pm 2)$ modulo 11, so the solutions are 5 and 3. Thus the solutions modulo 11 are $1, 3, 5$.

Considering the polynomial $x^3 - 9x^2 + 23x - 15$ modulo 13 we get

$$x^3 + 4x^2 - 3x - 2 = (x-1)(x^2 + 5x + 2).$$

The solution to the quadratic is $\frac{-5 \pm \sqrt{25-8}}{2} = 7(-5 \pm \sqrt{17}) = 7(-5 \pm 2)$ modulo 13, so the solutions are 15 and 3. Thus we know that the solutions modulo 13 are also $1, 3, 5$.

Lastly, we need to use the Chinese remainder theorem to find solutions modulo 143. There will be a solution for each pair of congruences modulo 11 and 13; this means that there are 9 solutions in all. Notice that

$$1 = 6 \cdot 11 - 5 \cdot 13.$$

We can use this to find the solutions via the Chinese Remainder Theorem; we find that the solutions to this polynomial are $1, 3, 5, 14, 16, 27, 122, 133, 135$.

(2) (a) We will prove this by induction on r, the number of equivalences. For $r = 1$ the theorem is obvious, and for $r = 2$ it is the Chinese Remainder Theorem, which was shown in class. We thus just need to prove the induction step. Suppose that for $r - 1$ relations the extended thoerem holds. Now consider r relations, as stated in the problem. By the induction hypothesis we know that there exists a unique value a modulo $m = m_1 \cdots m_{r-1}$ such that $x \equiv a \pmod{m}$. Now consider m and m_r. We know that they are relatively prime, since the m_i were pairwise relatively prime. Thus, by the Chinese Remainder Theorem there exists a unique b such that $x \equiv b \pmod{mm_r}$. This is a solution to the original equivalences, since $b \equiv a \pmod{m}$, so $b \equiv a_i \pmod{m}_i$ for $i < r$ (by the induction hypothesis) and $b \equiv a_r \pmod{m}_r$ by construction. Notice that we have constructed a solution to the system of r equivalences we were given. We simply need to prove that it is unique.

Suppose that there were two solutions M and N. Since they are the same modulo each m_i we know that $m_i | M - N$. But since the m's are pairwise relatively prime we know that $m_i | M - N$ for all i implies $m_1 \cdots m_r | M - N$, so $M \equiv N \pmod{m_1 \cdots m_r}$, as desired.

(b) We know that $20 = 2^2 \cdot 5$, $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$. Thus their least common multiple will be $2^2 \cdot 3^2 \cdot 5$. Notice that from the given equations it follows that

$$\begin{aligned} x &\equiv 13 \pmod{20} \qquad \text{from the first one} \\ x &\equiv -1 \pmod{9} \qquad \text{from the third one} \end{aligned}$$

We can solve these modulo 180, the least common multiple of these numbers (and also the original numbers). If the original equations have any solutions they must also satisfy the equations above; since the above equations have exactly one solution there is at most one solution to the given equation.
Solving the above equations modulo 180, we get that

$$x \equiv 53 \pmod{180}.$$

This works for the original equations, so it is the solution.
An alternate solution is just to write out all numbers between 0 and 180 that could work. This is not that much work (you start with 9 numbers and eliminate the impossible ones), since the information that the number is 13 modulo 20 reduces the possible numbers significantly.

(3) (a) Let $x = 2p_1 \cdots p_n$. Then

$$x^2 + 1 \equiv 4(p_1 \cdots p_n)^2 + 1 \equiv 0 \pmod{n}.$$

Since the equation has a solution modulo n, we know that it has a solution modulo any prime divisor of n; in particular, we know that it has a solution modulo p.

(b) We will show that p is of the form $4k+1$. This will prove that there are infinitely many primes of the form $4k+1$, since given any n such primes we can generate one that is not among those (since n is not divisible by any p_i).
Notice that $|(\mathbf{Z}/p)^\times| = p - 1$. If we can show that $4|p-1$ we will be done. In particular, if we can show that there exists an element whose order is divisible by 4 we will be done, since the order of any element divides the order of the group. Consider the element x defined in (a). We know that x satisfies $x^2 + 1 = 0$, so $x^2 = -1$. However, this means that $x^4 = 1$, and that this is the smallest such number. Thus $4 \mid \operatorname{ord}(x) \mid p-1$, so we are done.

(4) (a) First, notice that for all n such that an odd prime $p|n$, $\varphi(n)$ is even. This is because

$$\varphi(n) = \prod_{p^\alpha | n, p^{alpha+1} \not| n} (p-1)p^{\alpha-1},$$

so in particular $p-1$, which is even, divides $\varphi(n)$. At the same time, we know that if $2^i|n$ then $2^{i-1}|n$, which means that if $i > 1$ then $\varphi(n)$ is even.
Thus the only numbers n that could have $\varphi(n)$ odd are the ones that are divisible by no primes or just by 2, exactly once. These are just 1 and 2.

(b) We present two solutions. The first is more useful in the third part of this problem; the second one is a prettier bound.
First, notice that if $p > k+1$ and $p|n$, then $\varphi(n) > k$. This is because $p-1|\varphi(n)$, therefore $\varphi(n) \geq p - 1 > k$. Second, notice that if $\varphi(p^\alpha) > k$ and $p^\alpha|n$ then $\varphi(n) > k$; the reasoning is the same as above. In particular, the first observation

gives us a bound on the primes that can divide n that have $\varphi(n) \leq k$, and the second gives us a bound on the powers of a prime that can divide n. Thus we have only a finite number of different prime powers that can divide each such value of n, and thus a finite number of n such that $\varphi(n) \leq k$; from this it trivially follows that there is a finite number of n such that $\varphi(n) = k$.
Second: Notice that for any $p > 2$, $\varphi(p^\alpha) = (p-1)p^{\alpha-1} \geq \sqrt{p^\alpha}$. Also, for any $\alpha > 1$, $\varphi(2^\alpha) = 2^{\alpha-1} \geq \sqrt{2^\alpha}$. Also, notice that for relatively prime m, n not divisible by only one power of two we have

$$\varphi(mn) = \varphi(m)\varphi(n) \geq \sqrt{m}\sqrt{n} = \sqrt{mn}.$$

Thus for all n not divisible by exactly one power of two, $\varphi(n) \geq \sqrt{n}$.
We know that for $n = 2m$, with m odd, $\varphi(n) = \varphi(m)$, so we know from the above that $\varphi(n) \geq \sqrt{n/2}$. Since $\sqrt{n} > \sqrt{n/2}$ we can conclude that for all n,

$$\varphi(n) \geq \sqrt{n/2}.$$

However, this means that for $n > 2k^2$, $\varphi(n) > k$, so there are only finitely many n such that $\varphi(n) \leq k$.

(c) Consider the first description in part (b). We know that if $n = p^\alpha$ then $\varphi(n) = (p-1)p^{\alpha-1}$; if $n = mm'$ with $m, m' > 1$ and $(m.m') = 1$ then $\varphi(n) = \varphi(m)\varphi(m')$. This gives us a way to compute all n such that $\varphi(n) = k$. In particular, do it by induction: build up all divisors of k. Check whether there are $n = p^\alpha$ such that $\varphi(n) = k$ (this is not hard — these need to either be one more than k or they need to divide k). Then check if there are pairs of relatively prime m, m' such that $\varphi(m)\varphi(m') = k$. Following this algorithm, we construct the following table:

k	n such that $\varphi(n) = k$
1	$1, 2$
2	$3, 4, 2 \cdot 3 = 6$
3	none
4	$5, 8, 2 \cdot 5 = 10, 3 \cdot 4 = 12$
6	$7, 9, 2 \cdot 7 = 14, 2 \cdot 9 = 18$
8	$16, 3 \cdot 5 = 15, 3 \cdot 8 = 24, 3 \cdot 10 = 30, 4 \cdot 5 = 20, 6 \cdot 5 = 30$
12	$13, 2 \cdot 13 = 26, 3 \cdot 7 = 21, 3 \cdot 14 = 42, 4 \cdot 7 = 28, 4 \cdot 9 = 36$
24	$3 \cdot 13 = 39, 3 \cdot 26 = 78, 3 \cdot 28 = 84, 4 \cdot 13 = 52, 5 \cdot 7 = 35, 5 \cdot 9 = 45, 5 \cdot 14 = 70, 5 \cdot 18 = 90, 8 \cdot 7 =$

Notice that we know that we have found all values, since if $\varphi(n) = k$ then either n is a prime power (the numbers at the beginning of the row not in an equation) or n is composite, which means it is the product of two smaller numbers which are relatively prime; we have checked all such possible combinations. Thus the answer to the problem is

$$35, 39, 45, 52, 56, 70, 72, 78, 84, 90.$$

(5) (a) We first show how to properly expand a monomial $(x + tp^j)^m$. Notice that modulo p^{j+1} $p^{kj} \equiv 0$ for $k > 1$. Thus we only need to keep track of the terms

that are constant or linear in t; all of the other ones are zero. Thus

$$(x+tp^j)^m = x^m + \binom{m}{1}x^{m-1}tp^j + \sum_{k=2}^{m}\binom{m}{k}x^{m-k}t^m p^{kj}.$$

Notice that all terms in the sum are zero, since each binomial coefficient is an integer, and each p is taken to a power higher than $j+1$. Thus

$$(x+tp^j)^m = x^m + mx^{m-1}tp^j = x^m + (x^m)'tp^j pmodp.$$

Thus we have shown that for a monomial g we have $g(x+tp^j) = g(x)+g'(x)tp^j$. However, since a polynomial is a linear sum of monomials, and the derivative is linear, we know that

$$f(x+tp^j) = f(x) + f'(x)tp^j \pmod p.$$

Plugging in $x = a$ we get

$$f(a+tp^j) = f(a) + f'(a)tp^j \pmod p,$$

as desired.

(b) Since $f(a) = 0 \pmod{p^j}$ we know that $f(a) = kp^j$ for some integer k. Similarly, since $f(a+tp^j) = f(a)+f'(a)tp^j \pmod{p^{j+1}}$ we know that $f(a+tp^j) = f(a)+f'(a)tp^j + mp^{j+1}$ for some integer m.
A solution t to $f(a+tp^j) = 0 \pmod{p^{j+1}}$ is an integer t such that $f(a+tp^j) = np^{j+1}$. Plugging in from above for $f(a+tp^j)$ we see that we want a t such that

$$f(a) + f'(a)tp^j + mp^{j+1} = np^{j+1}.$$

We can simplify this to

$$f'(a)t = -\frac{f(a)}{p^j} + (n-m)p.$$

Notice that we can write $t = t_0 + bp$, with $0 \le t_0 \le p-1$ and b an integer. Thus we have

$$f'(a)t_0 + bpf'(a) = -\frac{f(a)}{p^j} + (n-m)p.$$

If we can find a t_0 such that this holds for some n, m, b, we can find a t such that $f(a+tp^j) \equiv p \pmod{p^j}$, since all of the steps above are reversible. However, the above equation is equivalent to

$$f'(a)t_0 \equiv -\frac{f(a)}{p^j} \pmod p$$

as desired.
We know that $\frac{f(a)}{p^j} = k$, and that $f'(a) \neq 0$. Thus we want to find all t_0 such that

$$f'(a)t_0 \equiv -k \pmod p.$$

Since $f'(a)$ is nonzero this is a linear equation in p over $\mathbf{Z}/p$, so it has exactly one solution.

(c) For this part of the problem we have $f'(a) = kp$.

(i) We claim that if $f(a) \equiv 0 \pmod{p^{j+1}}$ and $f'(a) \equiv 0 \pmod{p}$ then for all t_0 we will have $f(a+tp^j) \equiv 0$ modulo p^{j+1}. Indeed, from part (b) we know that $f(a+tp^j) \equiv f(a)+f'(a)tp^j \pmod{p^{j+1}}$. From the above equivalences we know that $f(a) = \ell p^{j+1}$; plugging this into the above equation we get

$$f(a+tp^j) \equiv f(a) + tp^j f'(a) \equiv \ell p^{j+1} + tp^j(kp) \equiv (\ell + tk)p^{j+1} \equiv 0 \pmod{p^{j+1}}.$$

Notice that this is independent of the value of t. Thus there is a lift for each value of t, so there are p lifts.

(ii) Now we suppose that $f(a) \not\equiv 0 \pmod{p^{j+1}}$. Again, expanding the equation we get

$$f(a+tp^j) \equiv f(a) + tp^j f'(a) \equiv f(a) \not\equiv 0 \pmod{p^{j+1}}.$$

This is once again independent of t. However, this time it is nonzero, so there can be no lifts to p^{j+1}.

(6) Consider the first equation modulo 7; it has the solutions 1 and -2. We know that $(x^2+x+47)' = 2x+1$. Let $a = 1$. Then $f(a) = 1+1+47 = 49 = 7 \cdot 7$, and $f'(a) = 3$. Thus $f(a)/7 = 7$, so from the formula in 5(b) we know that $t = 7 \cdot 3^{-1} \pmod 7 = 0$. Thus we have a solution $a = 1$ for x^2+x+47 modulo 49. If $a = -2$ then $f(a) = 4-2+47 = 49 = 7 \cdot 7$ and $f'(a) = -3$. However, because $k = 7$ we still have $t = 0$, and so the lifted solution is $a = 2$.

Now consider the equation modulo 7^3, We know that $f(a)/7^2 = 1$ for both roots. $f'(1) = 3$ and $f'(-2) = -3$. Thus we know that t for $a = 1$ is $-1 \cdot 3^{-1} \equiv (-1)(-2) \equiv 2 \pmod 7$. The t for $a = -2$ is $-1 \cdot (-3)^{-1} \equiv 3 \pmod 7$. Thus we have the two solutions

$$x = 1 + 2 \cdot 49 = 99 \qquad x = -2 + 3 \cdot 49 = 145.$$

Now consider the second equation. Modulo 9 we have solutions $x = 1$, $x = 4$ and $x = -2$ (as above). The values of $f'(a)$ are 3, 0, and -3, which are all 0 mod 3. Notice that $f(1) = 9$, $f(4) = 27$, and $f(-2) = 9$. Thus the only one of these for which lifts exist is 4, and there are three lifts for it. In particular, we see that the roots are $4, 13, 22$.