CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Satish Rao and Kannan Ramchandran

HW 5

Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up. (*signature here*)

1 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p,q,r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

Solution:

$N = pqr$ where p,q,r are all prime. Then, let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N,e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. I decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$ and thus $x^{ed} \equiv x \pmod{N}$. To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get $x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. As a reminder, we are considering the number: $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$.

We now argue that this number must be divisible by p, q, and r. Thus it is divisible by N and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- If x is divisible by p, then the entire thing is divisible by p.

- If x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

The same reasoning shows that it is divisible by q and r.

2 Breaking RSA

(a) Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N). Assume Eve has a friend Wolfram, who can easily return the roots of polynomials over $\mathbb{R}$ (this is, in fact, easy).

(b) When working with RSA, it is not uncommon to use $e = 3$ in the public key. Suppose that Alice has sent Bob, Carol, and Dorothy the same message indicating the time she is having her birthday party. Eve, who is not invited, wants to decrypt the message and show up to the party. Bob, Carol, and Dorothy have public keys $(N_1, e_1), (N_2, e_2), (N_3, e_3)$ respectively, where $e_1 = e_2 = e_3 = 3$. Furthermore assume that N_1, N_2, N_3 are all different. Alice has chosen a number $0 \le x < \min\{N_1, N_2, N_3\}$ which indicates the time her party starts and has encoded it via the three public keys and sent it to her three friends. Eve has been able to obtain the three encoded messages. Prove that Eve can figure out x. First solve the problem when two of N_1, N_2, N_3 have a common factor. Then solve it when no two of them have a common factor. Again, assume Eve is friends with Wolfram as above.

Hint: The concept behind this problem is the Chinese Remainder Theorem: Suppose $n_1, \ldots, n_k$ are positive integers, that are pairwise co-prime. Then, for any given sequence of integers $a_1, \ldots, a_k$, there exists an integer x solving the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions x of the system are congruent modulo the product, $N = n_1 \cdots n_k$. Hence: $x \equiv y \pmod{n_i}$ for $1 \le i \le k \iff x \equiv y \pmod{N}$.

Solution:

(a) Let $a = (p-1)(q-1)$. If Eve knows $a = (p-1)(q-1) = pq - (p+q) + 1$, then she knows $p + q = pq - a + 1$ (note that $pq = N$ is known too). In fact, p and q are the two roots of polynomial $f(x) = x^2 - (p+q)x + pq$ because $x^2 - (p+q)x + pq = (x-p)(x-q)$. Since she knows $p+q$ and pq, she can give the polynomial $f(x)$ to Wolfram to find the two roots of $f(x)$, which are exactly p and q.

Alternate Solution: Consider the polynomial $r(x) = (x-p)(x-q)$. Evaluate the polynomial at three special points.

$$\begin{aligned} r(0) &= N \\ r(1) &= (p-1)(q-1) \\ r(N) &= N(p-1)(q-1) \end{aligned}$$

Use polynomial interpolation to find the polynomial that goes through the three points $(0,N)$, $(1,(p-1)(q-1))$, $(N,N(p-1)(q-1))$, and then ask Wolfram for the roots of the polynomial.

(b) Eve first tests the GCD of all pairs of N_1, N_2, N_3. Let $d_1 = \gcd(N_1, N_2)$, $d_2 = \gcd(N_2, N_3)$, and $d_3 = \gcd(N_1, N_3)$. Then there are two cases:

case 1 If one of the d_1, d_2, or d_3 is greater than 1, it must be one of the prime factors p of the two N_i's. The other prime factor q can be recovered by $q = N_i/p$. Therefore, we can factorize one of the N_i's and once we do that, RSA is broken.

case 2 If $d_1 = d_2 = d_3 = 1$, it means all pairs of the N_i's are coprime. Let the three encoded messages be y_1, y_2, y_3. Since the messages are encoded by RSA with public keys $(N_1, 3)$, $(N_2, 3)$, and $(N_3, 3)$, we have:

$$\begin{aligned} x^3 &\equiv y_1 \pmod{N_1} \\ x^3 &\equiv y_2 \pmod{N_2} \\ x^3 &\equiv y_3 \pmod{N_3} \end{aligned}$$

Since all pairs of N_1, N_2, N_3 are coprime, by using the Chinese Remainder Theorem, we can solve the above system of congruence equations. Let the solution be

$$x^3 \equiv x_0 \pmod{N_1 N_2 N_3}$$

with $0 \le x_0 < N_1 N_2 N_3$. Since $x < N_1, N_2, N_3$, $x^3 < N_1 N_2 N_3$, and thus $x^3 = x_0$. We can take the cube root of x_0 and recover the original message $x = x_0^{1/3}$. In this problem, the trick is that we were able to convert a problem of finding cube-roots mod a prime (which is hard) into finding cube-roots in the integers (which is easy).

3 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is relatively prime to p and p is prime.

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct, i.e. $x^{ed} \equiv x \pmod{N}$. You may assume that x is relatively prime to both p and q.

(c) Continuing the previous part, prove that the scheme is unbreakable, i.e. your scheme is at least as difficult as ordinary RSA.

Solution:

(a) Consider the set S of all numbers between 1 and p^2-1 (inclusive) which are relatively prime to p. Consider the map $f(x) = ax$, and let T be the image of S, i.e. $T = f(S)$. Since a is relatively prime to p, and therefore relatively prime to p^2, we know that $a^{-1} \pmod{p^2}$ exists, modulo p^2. Since the inverse exists, we know that $f(x)$ has an inverse map, and is therefore a bijection: $|S| = |T|$. To show that $S = T$, it suffices to show that $T \subseteq S$. But if $t \in T$, then $t = as$ for some $s \in S$ with s relatively prime to p^2. Since a is also relatively prime to p^2, then $as = t$ is also relatively prime to p^2. We have shown that $t \in T$ implies $t \in S$, so $T \subseteq S$ (and by the discussion above, $T = S$). Finally, observe that the product of the elements of S is the same as the product of the elements of T, so

$$\prod_{s\in S} s \equiv \prod_{t\in S} t \equiv a^{|S|} \prod_{s\in S} s \pmod{p^2}$$

so we can conclude that $a^{|S|} \equiv 1 \pmod{p^2}$. To conclude the argument, we show that $|S| = p(p-1)$. But there are p^2 numbers between 1 and p^2, and if we subtract the p multiples of p, we end up with $|S| = p^2 - p = p(p-1)$.

Alternate Solution: We can use Fermat's Little Theorem, combined with the Binomial Theorem, to get the result. Since $\gcd(a,p) = 1$ and p is prime, $a^{p-1} \equiv 1 \pmod{p}$, so we can write $a^{p-1} = \ell p + 1$ for some integer ℓ. Then,

$$(a^{p-1})^p = (\ell p + 1)^p = \sum_{i=0}^{p} \binom{n}{i} (\ell p)^i = 1 + p \cdot (\ell p) + \binom{p}{2} (\ell p)^2 + \cdots + (\ell p)^p,$$

and since all of the terms other than the first term are divisible by p^2, $a^{p(p-1)} \equiv 1 \pmod{p^2}$.

(b) By the definition of d above, $ed = 1 + kp(p-1)q(q-1)$ for some k. Look at the equation $x^{ed} \equiv x \pmod{N}$ modulo p^2 first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo q^2, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2q^2}$.

(c) We consider the scheme to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$. (Observe that knowing $p(p-1)q(q-1)$ is enough, because we can compute the private key with this information.) Suppose that the scheme can be broken; we will show how to break ordinary RSA. For an ordinary RSA public key $(N = pq, e)$, square N to get $N^2 = p^2q^2$. By our assumption that the squared RSA scheme can be broken, knowing p^2q^2 allows us to find $p(p-1)q(q-1)$. We can divide this by $N = pq$ to obtain $(p-1)(q-1)$, which breaks the ordinary RSA scheme. This proves that our scheme is at least as difficult as ordinary RSA.

Remark: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.

4 Badly Chosen Public Key

Your friend would like to send you a message using the RSA public key $N = (pq, e)$. Unfortunately, your friend did not take CS 70, so your friend mistakenly chose e which is *not* relatively prime to $(p-1)(q-1)$. Your friend then sends you a message $y = x^e$. In this problem we will investigate if it is possible to recover the original message x. Throughout this problem, assume that you have discovered an integer a which has the property that $a^{(p-1)(q-1)} \equiv 1 \pmod N$, and for any positive integer k where $1 \le k < (p-1)(q-1)$, $a^k \not\equiv 1 \pmod N$.

(a) Show that for any integer z which is relatively prime to N, z can be written as $a^k \pmod N$ for some integer $0 \le k < (p-1)(q-1)$. [*Hint*: Show that $1, a, a^2, \dots, a^{(p-1)(q-1)-1}$ are all distinct modulo N.]

(b) Show that if k is any integer such that $a^k \equiv 1 \pmod N$, then $(p-1)(q-1) \mid k$.

(c) Assume that y is relatively prime to N. By the first part, we can write $y \equiv a^\ell \pmod N$ for some $\ell \in \{0, \dots, (p-1)(q-1)-1\}$. Show that if k is an integer such that $(p-1)(q-1) \mid ek - \ell$, then $\tilde{x} := a^k$ satisfies $\tilde{x}^e \equiv y \pmod N$.

(d) Unfortunately the solution $\tilde{x}$ found in the previous part might not be the original solution x. Show that if $d := \gcd(e, (p-1)(q-1)) > 1$, then there are exactly d distinct integers $x_1, \dots, x_d$ which are all distinct modulo N such that $x_i^e = y$, $i = 1, \dots, d$. [*Hint*: You will probably find it helpful to use a as a tool here.]

Solution:

(a) Note first that a has an inverse $a^{(p-1)(q-1)-1}$ modulo N and so a is relatively prime to N. Consequently, all of the integer powers of a are also relatively prime to N. Suppose that for some integers $0 \le i < j < (p-1)(q-1)$ we have $a^i \equiv a^j \pmod N$. Then, $a^{j-i} \equiv 1 \pmod N$, but $1 \le j - i < (p-1)(q-1)$, which contradicts the defining property of a. Hence, $1, a, a^2, \dots, a^{(p-1)(q-1)-1}$ are all distinct. Note that there are $(p-1)(q-1)$ elements in the set $\{1, a, a^2, \dots, a^{(p-1)(q-1)-1}\}$, each element in the set is relatively prime to N, and there are a total of $(p-1)(q-1)$ numbers relatively prime to N (modulo N), so we conclude that

$$\{1, a, a^2, \dots, a^{(p-1)(q-1)-1}\} = \{\text{numbers in } 0, 1, \dots, N-1 \text{ relatively prime to } N\}.$$

(b) By the Division Algorithm we can write $k = s(p-1)(q-1) + r$ for some $s \in \mathbb{Z}$, where the remainder $r \in \{0, \dots, (p-1)(q-1)-1\}$. However, $1 \equiv a^k \equiv a^{s(p-1)(q-1)+r} \equiv a^r$, and by the defining property of a, we must have $r = 0$, i.e., $(p-1)(q-1) \mid k$.

(c) Since $(p-1)(q-1) \mid ek - \ell$, write $ek - \ell = m(p-1)(q-1)$ for some $m \in \mathbb{Z}$. Then, $\tilde{x}^e \equiv (a^k)^e \equiv a^{ek-\ell} a^\ell \equiv a^{m(p-1)(q-1)} y \equiv y \pmod N$.

(d) Let us consider what a solution x' to the equation $(x')^e \equiv y \pmod N$ must look like. In particular, we would like to relate x' to the solution $\tilde{x}$ found in the previous part. We can write $x' = \tilde{x} x' \tilde{x}^{-1}$, and then since $(x')^e \equiv y \pmod N$, we have $\tilde{x}^e (x' \tilde{x}^{-1})^e \equiv y \pmod N$, but since

$\tilde{x}^e \equiv y \pmod N$, we see that $(x'\tilde{x}^{-1})^e \equiv 1 \pmod N$. In other words, the solutions are of the form $\tilde{x}\omega_i$, for $i = 1, \dots, d$, where ω_i is a solution to $\omega_i^e \equiv 1 \pmod N$. Therefore, it suffices to focus on the solutions of the equation $\omega^e \equiv 1 \pmod N$.

We will take a diversion to explore the connection with another beautiful part of mathematics: the roots of unity. As an equation in the complex numbers, $\omega^e = 1$ has exactly e solutions, known as the **eth roots of unity**: $\omega = 1, \mathrm{e}^{2\pi\mathrm{i}/e}, \mathrm{e}^{2\cdot 2\pi\mathrm{i}/e}, \dots, \mathrm{e}^{(e-1)\cdot 2\pi\mathrm{i}/e}$, where i denotes the imaginary unit. If we let $\omega_e := \mathrm{e}^{2\pi\mathrm{i}/e}$, then the solutions are given by $1, \omega_e, \omega_e^2, \dots, \omega_e^{e-1}$, that is, they are given by powers of ω_e. Thus, ω_e is known as a **primitive eth root of unity**.

In this problem, we are not working over the complex numbers, but there is a similar structure for the solutions of $\omega^e \equiv 1 \pmod N$. Namely, we know that $a^{(p-1)(q-1)} \equiv 1 \pmod N$, so a is the analogue of a primitive root of unity in modular arithmetic! To visualize the situation, imagine placing the powers of a, namely, $1, a^2, a^3, \dots, a^{(p-1)(q-1)-1}$, on a circle, see Figure 1.

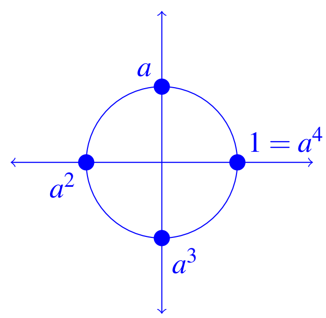

Figure 1: Here we demonstrate the primitive root of unity when $p = 2$, $q = 5$, so $(p-1)(q-1) = 4$. You can verify for yourself that 3 is a primitive root modulo $N = 10$. Multiplication by a corresponds to moving one hop counterclockwise on the circle, so that after four hops, we return back to the starting position; this corresponds to the equation $a^4 \equiv 1 \pmod{10}$. Similarly, multiplication by a^k, where $k \in \{0,1,2,3\}$, corresponds to a hop with a bigger step size, specifically, a hop which takes you k steps counterclockwise on the circle. We are looking for a solution to $\omega^e \equiv 1 \pmod{10}$. Because we know that all solutions ω have to be of the form a^k for some $k = \{0,1,2,3\}$, we are really asking: for what integers $k \in \{0,1,2,3\}$ does a^k return to itself after e hops, where each hop takes k steps? For example, if $e = 2$ in this example, then the powers of a which return to themselves after two hops are 1 and a^2.

After drawing a few more pictures and experimenting with other cases, we then conjecture that the solutions will be

$$\omega = a^{(p-1)(q-1)/d}, a^{2\cdot(p-1)(q-1)/d}, \dots, a^{(d-1)\cdot(p-1)(q-1)/d}.$$

Let us prove that this is the case formally. First observe that by the first part, the proposed solutions are all distinct. Next, to verify that the proposed solutions are indeed solutions, observe that

$$(a^{j(p-1)(q-1)/d})^e \equiv (a^{e/d})^{j(p-1)(q-1)} \equiv 1 \pmod N$$

because for any integer z which is relatively prime to N, $z^{(p-1)(q-1)} \equiv 1 \pmod N$ (this is part of the proof of correctness of RSA). Finally, we must show that there are no other solutions. Indeed, for any solution ω to $\omega^e \equiv 1 \pmod N$, we can write $\omega = a^m$ for some positive integer m, $0 \le m < (p-1)(q-1)$. By the Division Algorithm, we can write $m = q((p-1)(q-1)/d) +$

r for some integer q and $r \in \{0, \ldots, (p-1)(q-1)-1\}$. Then, since $\omega^e \equiv 1 \pmod{N}$,

$$1 \equiv \omega^e \equiv (a^{q(p-1)(q-1)/d+r})^e \equiv (a^{q(p-1)(q-1)/d})^e a^{er} \pmod{N}$$

and thus $a^{er} \equiv 1 \pmod{N}$. By the second part, we know that $(p-1)(q-1) \mid er$, but this implies that $r = 0$. So, $(p-1)(q-1)/d \mid m$, which means there are no other solutions other than the ones we proposed.

Closing Remarks: Such an integer a is called a **primitive root modulo** N. As you can see, the mere existence of a primitive root can lead to very fruitful results, because the primitive root tells you that the structure of your numbers under multiplication is **cyclic** (see Figure 1 for the visual intuition). Unfortunately, it is a fact that for the RSA scenario where $N = pq$, a primitive root modulo N exists only if one of the two primes is 2.

5 Properties of GF(p)

(a) Show that, if $p(x)$ and $q(x)$ are polynomials over the reals (or complex, or rationals) and $p(x) \cdot q(x) = 0$ for all x, then either $p(x) = 0$ for all x or $q(x) = 0$ for all x or both. (*Hint*: You may want to prove first this lemma, true in all fields: The roots of $p(x) \cdot q(x)$ is the union of the roots of $p(x)$ and $q(x)$.)

(b) Show that the claim in part (a) is false for finite fields GF(p).

Solution:

(a) First, notice that if r is a root of $p(x)$ such that $p(r) = 0$, then r must also be a root of $p(x) \cdot q(x)$, since $p(r) \cdot q(r) = 0 \cdot q(r) = 0$. The same is true for any roots of $q(x)$. Also notice that if some value s is neither a root of $p(x)$ nor $q(x)$, such that $p(s) \neq 0$ and $q(s) \neq 0$, then s cannot be a root of $p(x) \cdot q(x)$ since $p(s) \cdot q(s) \neq 0$. We therefore conclude that the roots of $p(x) \cdot q(x)$ is the union of the roots of $p(x)$ and $q(x)$.

Now we will show the contrapositive. Suppose that $p(x)$ and $q(x)$ are both non-zero polynomials of degree d_p and d_q respectively. Then $p(x) = 0$ for at most d_p values of x and $q(x) = 0$ for at most d_q values of x. This implies that $p(x) \cdot q(x)$ has at most $d_p + d_q$ roots. Since there are an infinite number of values for x (because we are using complex, real, or rational numbers) we can always find an x, call it $x_{\text{not zero}}$, for which $p(x_{\text{not zero}}) \neq 0$ and $q(x_{\text{not zero}}) \neq 0$. This gives us $p(x_{\text{not zero}}) \cdot q(x_{\text{not zero}}) \neq 0$ so pq is non-zero.

(b) In GF(p) where p is prime, $x^{p-1} - 1$ and x are both non zero polynomials, but their product, $x^p - x$ is zero for all x by Fermat's Little Theorem.

Examples for a specific p are also acceptable. For example, for GF(2), $p(x) = x$ and $q(x) = x + 1$.

6 Repeated Roots

Let $p(x) = a_k x^k + \cdots + a_0$ be a polynomial in the variable x, where k is a positive integer and the coefficients $a_0, \ldots, a_k$ are from some field F (here, F can be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathrm{GF}(p)$ for some prime p). We formally define the polynomial's **derivative** to be the polynomial $p'(x) := k a_k x^{k-1} + \cdots + a_1 = \sum_{j=1}^{k} j a_j x^{j-1}$. [Note: You may be familiar with the derivatives of polynomials from studying calculus, but we are not using any calculus here, because it does not really make sense to perform calculus on finite fields! Think of the polynomial's derivative as a formal definition, i.e., in this context, it has nothing to do with rate of change, etc. In particular, you should not use any calculus rules such as the product rule without proof.] We say that α is a **repeated root of** p if $p(x)$ can be factored as $(x-\alpha)^2 q(x)$ for some polynomial q. Show that α is a repeated root of p if and only if $p(\alpha) = p'(\alpha) = 0$.

Solution:

Here we use the fact that α is a root of p if and only if $p(x) = (x-\alpha)r(x)$ for some polynomial r.

If α is a repeated root of p, then $p(x) = (x-\alpha)^2 q(x)$. Plugging in $x = \alpha$, we see that $p(\alpha) = 0$. Note that if $q(x) = \sum_{j=0}^{m} b_j x^j$ for some $m \in \mathbb{N}$, then

$$\begin{aligned}
p(x) &= (x^2 - 2\alpha x + \alpha^2) \sum_{j=0}^{m} b_j x^j = \sum_{j=0}^{m} b_j (x^{j+2} - 2\alpha x^{j+1} + \alpha^2 x^j), \\
p'(x) &= \sum_{j=1}^{m} b_j \big((j+2) x^{j+1} - 2\alpha (j+1) x^j + \alpha^2 j x^{j-1} \big) + b_0 (2x - 2\alpha), \\
p'(\alpha) &= \sum_{j=1}^{m} b_j \big((j+2) \alpha^{j+1} - 2(j+1) \alpha^{j+1} + j \alpha^{j+1} \big) = 0.
\end{aligned}$$

Conversely, if $p(\alpha) = p'(\alpha) = 0$, then α is a root of p and we can write $p(x) = (x-\alpha)r(x)$. Write $r(x) = \sum_{j=0}^{\ell} c_j x^j$ for some non-negative integer ℓ. Then,

$$\begin{aligned}
p(x) &= (x-\alpha) \sum_{j=0}^{\ell} c_j x^j = \sum_{j=0}^{\ell} c_j (x^{j+1} - \alpha x^j), \\
p'(x) &= \sum_{j=1}^{\ell} c_j \big((j+1) x^j - \alpha j x^{j-1} \big) + c_0, \\
p'(\alpha) &= \sum_{j=1}^{\ell} c_j \big((j+1) \alpha^j - j \alpha^j \big) + c_0 = \sum_{j=1}^{\ell} c_j \alpha^j + c_0 = r(\alpha) = 0,
\end{aligned}$$

and so α is a root of r. That means r can be factored as $r(x) = (x-\alpha)\tilde{q}(x)$ for some polynomial $\tilde{q}(x)$, and hence $p(x) = (x-\alpha)^2 \tilde{q}(x)$.