1 (5 points). Suppose that \( n \) and \( m \) are positive integers, that \( p \) is a prime and that \( \alpha \) is a non-negative integer. Assume that \( n \) is divisible by \( p^\alpha \), that \( m \) is prime to \( p \) and that \( F = \frac{n}{m} \) is an integer. Show that \( F \) is divisible by \( p^\alpha \).

This is an abstraction of the situation of problem #14 on page 63, where some students had trouble exploiting the hint. The integer \( Fm \) is divisible by \( p^\alpha \), and \( m \) is prime to \( p \). This means that \( \gcd(m, p^\alpha) = 1 \). Since \( p^\alpha | nF \) and \( \gcd(m, p^\alpha) = 1 \), we may conclude that \( p^\alpha \) divides \( F \) by Th. 1.10 on p. 10.

2 (6 points). Let \( f(x) \) be a polynomial with integer coefficients that satisfies \( f(1) = f'(1) = 3 \). Calculate the remainder when \( f(-18) \) is divided by \( 19^2 \).

By Taylor’s theorem, \( f(-18) = f(1 - 19) = f(1) - f'(1) \cdot 19 + \text{terms that are divisible by } 19^2 \). Hence the answer is \(-3 \cdot 18 = -54 \mod 85\); we should say “\( 19^2 - 54 = 307 \)” because we want the answer to be positive here.

3 (5 points). Determine the number of solutions to the congruence \( x^2 + x + 1 \equiv 0 \mod 7^{11} \).

Modulo 7, there are the two solutions 2 and 4. These are both non-singular, since \( 2x + 1 \) is non-zero mod 7 when \( x = 2 \) and \( x = 4 \). Hensel’s lemma implies that each solution lifts uniquely mod \( 7^n \) for \( n = 1, 2, \ldots \). Thus the answer is “two”.
4 (6 points). Find an integer \( n \geq 1 \) so that \( a^{3n} \equiv a \mod 85 \) for all integers \( a \) that are divisible neither by 5 nor by 17.

This is an RSA-related problem, although RSA is not mentioned explicitly. By Euler’s theorem, it suffices to find an inverse to 3 \mod \varphi(85) = 64. Since \( 3 \cdot 43 = 129 \equiv 1 \mod 64 \), we can take \( n = 43 \). Actually, as several of you noted, one can take \( n = 11 \) instead; if you didn’t give “11” as your answer, you should check why this number works.

5 (6 points). Find the number of solutions mod 120 to the system of congruences:

\[
\begin{align*}
x &\equiv 2 \mod 4 \\
x &\equiv 3 \mod 5 \\
x &\equiv 4 \mod 6
\end{align*}
\]

The gcd of 4 and 6 is 12. Hence the first and third congruences determine \( x \) uniquely mod 12 if they are consistent. Since 2 and 4 have the same residue mod 2 = \gcd(4, 6), the two congruences are indeed consistent. They amount to the statement that \( x \) is 10 mod 12. Thus congruence, plus the second, gives a single congruence that \( x \) must satisfy mod 60; in fact, \( x \) has to be \(-2 \equiv 58 \mod 60\). Conclusion: there are two solutions mod 120, namely 58 and 118.

6 (7 points). If \( m = 15709 \), we have \( 2^{(m-1)/2} \equiv 1 \mod m \) and \( 2^{(m-1)/4} \equiv 2048 \mod m \). With the aid of these congruences, one can find quite easily a positive divisor of \( m \) that is neither 1 nor \( m \). Explain concisely: how to find such a divisor, and why your method works.

This is basically problem 9 on page 82, where we have \( x^2 \equiv 1 \mod m \) but \( x \not\equiv \pm 1 \mod m \). In this situation, we can’t have \( \gcd(1 + x, m) = 1 \). If this gcd were 1, we could exploit the divisibility \( m|((1 + x)(1 - x)) \) and conclude that \( m \) divides \((1 - x)\) by the theorem on p. 10 that was mentioned above. Since \( x \not\equiv 1 \mod m \), however, \( m \) does not divide \( x - 1 \). Also, \( \gcd(1 + x, m) \) is different from \( m \) because \( x \) is not \(-1 \mod m \). Thus \( \gcd(1 + x, m) \) is a non-trivial divisor of \( m \), i.e., a positive divisor that is different from 1 and \( m \). We’ve found a factor of \( m \)! The wording of the question does logically allow answers that have nothing to do with this method or with the given congruences; for example, you could suggest dividing \( m \) by all the numbers from 1 to \( \lfloor \sqrt{m} \rfloor \). I hope that no one gives an answer like this!

115 midterm—page2