The first three problems are related to the last few lectures. The last four problems are review problems.

1. a) We need the sequence

   \[ \begin{align*}
   x_0 &= 2 \\
   x_1 &= 5 \\
   x_2 &= 26 \\
   x_3 &= 677 \\
   x_4 &= 620 \\
   x_5 &= 202 \\
   x_6 &= 582.
   \end{align*} \]

   Note

   \[ \begin{align*}
   x_2 - x_1 &= 21 \\
   x_4 - x_2 &= 594 \\
   x_6 - x_3 &= -95
   \end{align*} \]

   and

   \[ \begin{align*}
   (x_2 - x_1, 1387) &= 1 \\
   (x_4 - x_2, 1387) &= 1 \\
   (x_6 - x_3, 1387) &= 19
   \end{align*} \]

   so 19 is a prime divisor of 1387, with \( 19 \cdot 73 = 1387 \). Since 73 is prime, we conclude that the prime factorization of 1387 is

   \[ 1387 = 19 \cdot 73. \]

   d) We need the sequence

   \[ \begin{align*}
   x_0 &= 2 \\
   x_1 &= 11 \\
   x_2 &= 1343 \\
   x_3 &= 767 \\
   x_4 &= 978.
   \end{align*} \]

   Note

   \[ \begin{align*}
   x_2 - x_1 &= 1332 \\
   x_4 - x_2 &= -365
   \end{align*} \]

   and

   \[ \begin{align*}
   (x_2 - x_1, 1387) &= 1 \\
   (x_4 - x_2, 1387) &= 73
   \end{align*} \]

   so 73 is a prime divisor of 1387, with \( 73 \cdot 19 = 1387 \). Since 73 is prime, we conclude that the prime factorization of 1387 is

   \[ 1387 = 19 \cdot 73. \]
2. We convert the phrase THE RIGHT CHOICE to numbers as follows:

\[
19 \ 7 \ 4 \ 17 \ 8 \ 6 \ 7 \ 19 \ 2 \ 7 \ 14 \ 8 \ 2 \ 4
\]

For each of these numbers \( P \), we compute the least positive residue of \( 15P + 14 \mod 25 \):

\[
15(2) + 14 \equiv 18 \mod 25 \\
15(4) + 14 \equiv 22 \mod 25 \\
15(6) + 14 \equiv 0 \mod 25 \\
15(7) + 14 \equiv 15 \mod 25 \\
15(8) + 14 \equiv 4 \mod 25 \\
15(14) + 14 \equiv 16 \mod 25 \\
15(17) + 14 \equiv 9 \mod 25 \\
15(19) + 14 \equiv 13 \mod 25
\]

Thus the ciphertext message is

\[
13 \ 15 \ 22 \ 9 \ 4 \ 0 \ 15 \ 13 \ 18 \ 15 \ 16 \ 4 \ 18 \ 22
\]

which in letters is

\[
N \ P \ W \ J \ E \ A \ P \ N \ S \ P \ Q \ E \ S \ W
\]

To decrypt with the affine cipher \( C \equiv 3P + 24 \mod 26 \), we use the transformation

\[
P \equiv 3(C - 24) \mod 26,
\]

where \( 3 = 9 \) is an inverse of 3 mod 27. In numbers, the message RTOLKTOIK reads

\[
17 \ 19 \ 14 \ 11 \ 10 \ 19 \ 14 \ 8 \ 10.
\]

For each of these numbers \( C \), we compute the least positive residue of \( 9(C - 24) \mod 25 \).

\[
9(8 - 24) \equiv 12 \mod 25 \\
9(10 - 24) \equiv 4 \mod 25 \\
9(11 - 24) \equiv 13 \mod 25 \\
9(14 - 24) \equiv 14 \mod 25 \\
9(17 - 24) \equiv 15 \mod 25 \\
9(19 - 24) \equiv 7 \mod 25
\]

Thus the plaintext message is

\[
15 \ 7 \ 14 \ 13 \ 4 \ 7 \ 14 \ 12 \ 4
\]

which in letters is

\[
PHONE \ HOME.
\]

3. This problem should have read \( a^{(m-1)/2} \not\equiv \pm 1 \mod m \). I will not be grading this problem at all now. I will go over the solution in class.
4. Any solution \( x \) to the polynomial congruence
\[
f(x) \equiv 0 \mod 162
\]
where \( f(x) = x^4 + 110x^3 + 458x^2 + 135x + 81 \), must also be a solution to
\[
f(x) \equiv 0 \mod 2.
\]
By inspection, we see that \( f(0) = 81 \not\equiv 0 \mod 2 \), and \( f(1) = 1 + 110 + 458 + 135 + 81 \not\equiv 0 \mod 2 \). Thus there are not solutions to \( f(x) \equiv 0 \mod 2 \), so there are not solutions to \( f(x) \equiv 0 \mod 162 \) either.

5. We show that a sum of squares can never be congruent to 3 mod 4. It will follow immediately from this that, in particular, a prime can not be a sum of two squares.
Consider \( n^2 + m^2 \). If \( n \) and \( m \) are both even or both odd, then \( n^2 + m^2 \) is even, so it’s congruent to either 0 or 2 mod 4. So suppose without loss of generality that \( n = 2k + 1 \) and \( m = 2l \). Then
\[
n^2 + m^2 = (2k + 1)^2 + 4l^2 = 4k^2 + 4k + 1 + 4l^2 = 4(k^2 + k + l^2) + 1,
\]
so \( n^2 + m^2 \) must be congruent to 1 mod 4. In particular, \( n^2 + m^2 \) can not be congruent to 3 mod 4.

6. We proceed by induction. For \( n \) strictly smaller than 6 and not equal to 2, we observe that
\[
\phi(1) = 1 \geq \sqrt{1},
\]
\[
\phi(3) = 2 \geq \sqrt{3},
\]
\[
\phi(4) = 2 \geq 2 = \sqrt{3},
\]
and
\[
\phi(5) = 4 \geq \sqrt{5},
\]
so the claim is true in these cases. We can also easily verify
\[
\phi(7) = 6 \geq \sqrt{7}.
\]
If \( n \) is strictly bigger than 6, then one of the following three possibilities must hold:

(i) \( 2^k \mid n \) for some \( k \geq 2 \),
(ii) \( 3^l \mid n \) for some \( l \geq 2 \), or
(iii) \( n \) has a prime divisor \( p \) larger than both 2 and 3.
For case (i), let \( k \geq 2 \) be the largest integer such that \( 2^k \mid n \). We can write \( n = 2^k m \) where 2 and \( m \) are coprime. Note \( m < n, m \neq 2 \) and \( m \neq 6 \) (because otherwise \( 2^{k+1} \mid n \)). Then by induction
\[
\phi(n) = \phi(2^k)\phi(m) \geq \phi(2^k)\sqrt{m}.
\]
Since \( k \geq 2 \),
\[
\phi(2^k)\sqrt{m} = 2^{k-1}(2-1)\sqrt{m} = 2^{k-1}\sqrt{m} \geq 2^\frac{k}{2}\sqrt{m} = \sqrt{2^k}\sqrt{m} = \sqrt{2^km} = \sqrt{n}.
\]
We conclude that \( \phi(n) \geq \sqrt{n} \) in this case.
Case (ii) is similar but a little more involved. Let \( l \geq 2 \) be the largest integer such that \( 3^l \mid n \). We can write \( n = 3^l a \) where \( 3 \) and \( a \) are coprime. Note \( a < n \), and \( a \neq 6 \). If furthermore we assume \( a \neq 2 \), then by induction, we have
\[
\phi(n) = \phi(3^l) \phi(a) \geq \phi(3^l) \sqrt{a}.
\]
Note
\[
\phi(3^l) \sqrt{a} = 3^{l-1}(3 - 1) = 2 \cdot 3^{l-1} \sqrt{a}.
\]
Suppose for a contradiction that \( 2 \cdot 3^{l-1} < \sqrt{3^l} = 3^{l/2} \). Then
\[
\frac{3^{l-1}}{3^{l/2}} = 3^{l-1-\frac{l}{2}} = 3^{l/2} < \frac{1}{2},
\]
so we must have
\[
\frac{l - 2}{2} < 0,
\]
implying that \( l < 2 \), which is a contradiction. Thus \( 2 \cdot 3^{l-1} \geq \sqrt{3^l} \) and we conclude that
\[
\phi(n) \geq \phi(3^l) \sqrt{a} \geq \sqrt{3^l \sqrt{a}} = \sqrt{3^l a}.\]

On the other hand (still in case (ii)), suppose \( a = 2 \). Then \( \phi(n) = \phi(3^l \cdot 2) = \phi(3^l) \) where \( l \geq 2 \). We need to show \( \phi(3^l) = 3^{l-1} \cdot 2 \geq \sqrt{n} = \sqrt{3^l \cdot 2} = 3^{l/2} 2^{1/2} \). Suppose otherwise: the inequality
\[
3^{l-1} \cdot 2 > 3^{l/2} 2^{1/2}
\]
is equivalent to
\[
2^{1/2} > 3^{(l/2) - l + 1} = 3^{(2-l)/2}.
\]
Clearly \( 2^{1/2} > 3^{1/2} \), so
\[
3^{(2-l)/2} > 3^{l/2},
\]
which upon squaring shows
\[
3^{2-l} > 3^l
\]
hence \( l < 2 - l \), contradicting that \( l \geq 2 \). We conclude that \( \phi(n) \geq \sqrt{n} \).

Finally, consider case (iii), in which \( n \) has a prime divisor \( p \) greater than 3. Write \( n = p^j b \) where \( p \) and \( b \) are coprime. Then \( \phi(n) = \phi(p^j) \phi(b) \). If \( b \neq 2 \) and \( b \neq 6 \), induction shows
\[
\phi(n) \geq \sqrt{p^j b} = \sqrt{n}.
\]
Suppose \( b = 2 \). We need to show \( \phi(n) = p^{j-1}(p - 1) \geq \sqrt{n} = p^{j/2} \cdot 2^{1/2} \). Suppose otherwise. Then, we have
\[
p^{j-1}(p - 1) < p^{j/2} \cdot 2^{1/2},
\]
which is equivalent to
\[
p^{(j-2)/2}(p - 1) < 2^{1/2},
\]
which upon squaring shows
\[
p^{j-2}(p - 1)^2 = p^{j-2}(p^2 - 2p + 1) < 2.
\]
If \( j > 1 \), then, since \( p \) is a prime greater than 3
\[
p^{j-2}(p^2 - 2p + 1) > 5^2 - 10 + 1 = 16,
\]
which is clearly bigger than 2. We conclude \( j = 1 \), in which case
\[
p^{-1}(p^2 - 2p + 1) > n^{-1}(p^2 - 2p) = p - 2 \geq 5 - 2 = 3,
\]
yielding the contradiction $3 < 2$. Therefore $\phi(n) \geq \sqrt{n}$ when $n = 2 \cdot p^j$.

If $b = 6$, then $\phi(n) = \phi(p^j 6) = \phi(p^j) \phi(2) = 2\phi(p^j) = 2p^{j-1}(p - 1)$. We need to show $2p^{j-1}(p - 1) \geq \sqrt{n} = 2^{1/2}p^{j/2}$. Suppose otherwise, so that

$$2p^{j-1}(p - 1) < 2^{1/2}p^{j/2}.$$  

Squaring both sides yields

$$4p^{2j-2}(p - 1)^2 = 4p^{2j-2}(p^2 - 2p + 1) < 2p^j.$$  

Dividing through by $2p^j$ yields

$$2p^{j-2}(p^2 - 2p + 1) < 1$$  

which can’t hold because $p > 3$ and $j > 0$. We conclude that $\phi(n) \geq \sqrt{n}$ in case (iii). This completes the proof of the claim.

7. It does not matter that $p$ and $q$ are coprime, as our proof now shows. Consider the prime power factorizations

$$a = p_1^{j_1} \cdots p_m^{j_m}$$  

and

$$b = q_1^{l_1} \cdots q_n^{l_n}.$$  

Since $a^p \mid b^q$, we have that for all $a = 1, \ldots, m$, $p_a = q_b$ for some $b_a$ and $p_a \leq q_b$. Since $p > q$, $\frac{p}{q} < 1$, hence

$$j_a \leq q \frac{b_a}{p} \leq b_a.$$  

So for every $a = 1, \ldots, m$, $p_a = q_b$ for some $b_a$ and $j_a \leq b_a$. This implies $a \mid b$.  

5