# Answers 8

**Problem 1**
N = 221 = 13·17. Let $p = 13$ and $q = 17$. Then
for $m = 1$, $n = m\cdot(p-1)(q-1)/2 + 1 = 97$ (prime; $A = 77$ not a factor)
for $m = 2$, $n = m\cdot(p-1)(q-1)/2 + 1 = 193$ (prime; $A = 77$ not a factor)
for $m = 3$, $n = m\cdot(p-1)(q-1)/2 + 1 = 289 = 17\cdot17$ (prime squared; $A = 77$ not a factor)
for $m = 4$, $n = m\cdot(p-1)(q-1)/2 + 1 = 385 = 5\cdot7\cdot11$ ($A = 7\cdot11 = 77$ is a factor)
Therefore the other factor is $B = 5$. Then corresponding to

$x = 72,\ 284,\ 49,\ 2,\ 83,\ 186,\ 82,\ 57,\ 184,\ 90,\ 50$

we decrypt

$y = x^B \bmod N = 89,\ 97,\ 121,\ 32,\ 70,\ 101,\ 114,\ 109,\ 97,\ 116,\ 33$

From the ASCII table these $y$s correspond to

Y a y F e r m a t !

**Problem 2**
$A = 11941$ and $N = 16850989 = 4099\cdot4111 = p\cdot q$.
for $m = 1$, $n = m\cdot(p-1)(q-1)/2 + 1 = 8421391$. $8421391/A = 705.250...$ ($A$ not a factor)
for $m = 2$, $n = m\cdot(p-1)(q-1)/2 + 1 = 16842781$. $16842781/A = 1410.500...$ ($A$ not a factor)
for $m = 3$, $n = m\cdot(p-1)(q-1)/2 + 1 = 25264171$. $25264171/A = 2115.750...$ ($A$ not a factor)
for $m = 4$, $n = m\cdot(p-1)(q-1)/2 + 1 = 33685561$. $33685561/A = 2821 = B$.

**Problem 3**
$p = 5$ and $q = 13$. Then
for $m = 1$, $n = m\cdot(p-1)(q-1)/2 + 1 = 25 = 5\cdot5$ (prime squared)
for $m = 2$, $n = m\cdot(p-1)(q-1)/2 + 1 = 49 = 7\cdot7$ (prime squared)
for $m = 3$, $n = m\cdot(p-1)(q-1)/2 + 1 = 73$ (prime)
for $m = 4$, $n = m\cdot(p-1)(q-1)/2 + 1 = 97$ (prime)
for $m = 5$, $n = m\cdot(p-1)(q-1)/2 + 1 = 121$ (prime squared)
for $m = 6$, $n = m\cdot(p-1)(q-1)/2 + 1 = 145 = 5\cdot29 = A\cdot B$

**Problem 4**
Did your friend decrypt and decode your message?