60) Assume that you are using a RSA public key system with modulus $30053021 = 5003 \cdot 6007$ and exponent $e = 67$.
a) Encrypt the number 1234 using the RSA scheme.
b) You received the message 4673111. Decrypt it.

61) Consider an RSA encryption system with modulus m and exponent e such that $\gcd(e, \varphi(m)) = 1$.
a) Show that $\varphi(m)$-fold encryption returns a message to itself. (This means that $\varphi(m) - 1$-times encryption of an encrypted message decrypts it.)
b) As the encrypting mechanism is published it would be counterproductive if there was a small number k such that k-fold encryption returns a message to itself. (Because then repeated encryption could be used to decrypt a message.) Show that for a given e, this smallest k is given by $\mathrm{OrderMod}_{\varphi(m)}(e)$.
c) For modulus $30053021 = 5003 \cdot 6007$, find an exponent e with $k = 2$, that is encryption and decryption are the same process.

62) Let $R = \mathbb{Z}_3[x]$ the ring of all polynomials over $Z_3 = \mathbb{Z}/3\mathbb{Z}$, the integers modulo 3.
a) Let A be the set of all of these polynomials of degree < 2. Write a list of the elements of A.
b) Form an addition table (i.e. a 9×9 matrix) for the elements of A.
c) Let $p(x) = x^2 + 1$. Show that $p(x)$ has no zero in $\mathbb{Z}_3$. (We say that p is a prime element in R.)
d) We now define a multiplication on A with a product modulo p. Write down the multiplication table (E.g. $(x+1) \cdot (x-1) = x^2 - 1$, $x^2 - 1 = p(x) + 1$, so the product would be $(x+1)(x-1) \equiv 1 \pmod{p}$. Similarly $(x+1)(x+1) = x^2 - x + 1 = p(x) + x$, so $(x+1)^2 \equiv x \pmod{p}$.)
One can now show that with these operations A becomes a field (with 9 elements).

63) Show how an initial *decryption* of a given message with RSA can be used to prove (by encrypting with the public key) that a message was created by a particular person. (Thus a document can be signed electronically.)

64) One of the shortest talks ever was given at the 1903 meeting of the American Mathematical Society. Frank N. Cole went to the blackboard and calculated $2^{67} - 1$ as well as $193707721 \cdot 761838257287$. He sat down again without saying a word. The audience applauded, as a factorization of this number (that had been disproved to be a prime already in 1875 by E. Lucas) had been considered impossible for a long time. [1]
a) Prove that $2^{67} - 1$ is not prime (without referring to the factorization, i.e. show that it is not a pseudoprime).
b) Using the Miller-Rabin test, show that 193707721 is prime with probability more than $1 - 10^{10}$.

65) Let p and q be distinct odd primes, and let $n = pq$. Suppose that the integer x satisfies $\gcd(x, pq) = 1$. a) Show that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{p}$ and $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{q}$.
b) Using the Chinese Remainder Theorem, conclude that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$.
c) Show that if $ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$, then $x^{ed} \equiv x \pmod{n}$, that is one could use $\frac{1}{2}\varphi(n)$ to determine the decrypting exponent d.

66) Suppose the *same* message m has been encrypted twice with RSA for the same modulus n but different exponents e, f, that is you know n, e, f and $c_1 \equiv m^e \pmod{n}$, $c_2 \equiv m^f \pmod{n}$. Assuming that $\gcd(e, f) = 1$, show that you can recover m. (**Hint:** Consider products of the form $c_1^u \cdot c_2^v \bmod n$.)
This means that it is a good idea to not re-use the same modulus for RSA, even if the exponent is changed.

Practice Problems: **3.5**, **3.6**, **3.7**,

[1] Later, asked how long this factorization took him, Cole responded: "The sundays of three years"