25) Show that $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number.

Side remark:
One of the best-known anecdotes in the history of mathematics is about a visit that G.H.Hardy (for more historical information see `http://turnbull.mcs.st-and.ac.uk/history/Mathematicians/Hardy.html`) paid to his fellow number theorist S.A.Ramanujan (see `http://turnbull.mcs.st-and.ac.uk/history/Mathematicians/Ramanujan.html`) in the hospital in 1917. During one visit Hardy mentioned that the number of the taxi cab that had brought him was 1729, which, as numbers go, Hardy thought was "rather a dull one". At this, Ramanujan perked up, and said "No, it is a very interesting number; it is the smallest number expressible as a sum of two cubes in two different ways."

26) Find all positive integers n that fulfill:
a) $\varphi(n) = \varphi(2n)$
b) $\varphi(n) < \varphi(2n)$
c) $2\varphi(n) | n$

27)* (GAP) Find the smallest number k, such that there is no integer n with $\varphi(n) = k$. (Note that the prime factors of k limit the prime factors of n, similarly for the exponents. Use GAP to show that smaller numbers k can be obtained as $\varphi(n)$.)

28) Let p, q be primes and $n = pq$, $m = \varphi(n)$. Show that one can determine the values of p and q from the values of n and m without factorizing n.

29*) It may appear that the RSA decryption will not work, if you're unlucky enough to choose a message a that is not relatively prime to m. Of course, if $m = pq$ and p and q are large, this is unlikely to occur.
a) Show that in fact RSA decryption does work for all messages a, regardless of whether they have a factor in common with m.
b) More generally, show that RSA decryption works for all messages a as long as m is a product of distinct primes.
c) Give an example with $m = 18$ and $a = 3$ where RSA decryption does not work.

30) Suppose that $n = rs$ with $r, s > 2$ and $(r, s) = 1$. Show that

$$a^{\frac{\varphi(r)\varphi(s)}{2}} \equiv 1 \pmod{n},$$

that is $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$.

31) (GAP) In this problem we use the following translation table for letters and numbers:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

a) You have been sent the following message:

5272281348 21089283929 3117723025 26844144908 22890519533
26945939925 27395704341 2253724391 1481682985 2163791130
13583590307 5838404872 12165330281 28372578777 7536755222

It has been encoded using $p = 187963$, $q = 163841$, $m = pq = 30796045883$, $k = 48611$. Decode the message.

b*) (This part can be handed in until the end of the semester.) You intercept the following message, which you know has been encoded using the modulus

$$m = 956331992007843552652604425031376690367$$

and exponent $k = 12398737$. Break the code and decipher the message.

821566670681253393182493050080875560504
870741731290463997209497869585113910 52
552100909946781566365272088688468880029
491078995197839451033115784866534122828
172219665767314444215921020847762293421

You can find these numbers on the web page:
`http://www.math.brown.edu/~jhs/frintdir/FRINTExercise18.3.html`
to save you retyping.
Problems marked with a *are bonus problems for extra credit.