Math 467 Factorizaton and Primality Testing, Fall Term 2024
Practice Exam 1 Model Solutions.

Note: Exam 1 will be 9:05-9:55, Wednesday 25th September 2024 Room 012 Walker

1. Show that $n|(n-1)!$ for all composite $n > 4$.

We have $n = lm$ with $1 < l \leq m < n$. When $l \neq m$, both l and m occur in the product $(n-1)!$ and so $n = lm|(n-1)!$. When $l = m$, since $n > 4$ we have $l \geq 3$ and $l < 2l < l^2 = n$ so both l and $2l$ occur in the product $(n-1)!$.

2. (25 marks) Prove that if $m \in \mathbb{N}$ and $n \in \mathbb{N}$, then there are integers a, b such that $\gcd(a,b) = m$ and $[a,b] = n$ if and only if $m|n$.

If $m|n$, then let $a = m$ and $b = n$. Then $m|b$, so that $(a,b) = m$ and $[a,b] = ab/(a,b) = mn/m = n$. On the other hand if there are a, b with $(a,b) = m$ and $[a,b] = n$, then $m|a$ and $m|b$ so that $n = [a,b] = ab/(a,b) = (a/m)(b/m)m$, whence $m|n$.

3. (25 marks) Factorise 4087.

$4087 = 4096 - 9 = 2^{12} - 3^2 = (2^6 - 3)(2^6 + 3) = 61 \times 67.$

4. (25 marks) Find x and y such that $922x + 2163y = \gcd(922, 2163)$.

j	q_j	r_j	x_j	y_j
-1		2163	0	1
0	2	922	1	0
1	2	319	-2	1
2	1	284	5	-2
3	8	35	-7	3
4	8	4	61	-26
5	1	3	-495	211
6		1	556	-237

$\gcd(922, 2163) = 1 = 556 \times 922 + (-237) \times 2163$