1.

Цикл выполниться раз но так как n = e можно сказать что цикл выполнится раз.

Представим n в двоичном представлении то есть

n = где

Следовательно, дополнительное умножение будет выполняться столько же сколько единиц в двоичной записи числа n (Пусть будет S – единиц). Причем

Всего будет операций умножения.

Чтобы узнать всегда ли данный алгоритм лучше наивного способа вычисления, требующего в точности n умножений, решим неравенство:

Так как S в худшем случае равно n то неравенство будет:

Ответ:

То есть при наивный алгоритм будет эффективнее чем FAST EXPONENT.

2.

**INIT**: Перед началом цикла

**CONT**: Дано:

r1, p1, e1 – в начале итерации

r2, p2, e2 – в конце итерации

Доказать: не изменится.

▫ 1) Пусть e1 – четное число.

Тогда следовательно подходит.

2) Пусть e1 – нечетное число.

Тогда следовательно подходит. ▪

**EXIT**: Предпоследним значением e при любом условии будет 1, а после 0, следовательно при единице r будет умножено на последнее p, а дальнейшее умножение не будет иметь значения.